POWER TO THE PEOPLE: HOW BLOCKCHAIN BASED DIGITAL IDENTITY CAN EMPOWER DISADVANTAGED INDIVIDUALS

Hasan Syed

TC 660H
Plan II Honors Program
The University of Texas at Austin

6 May 2019

_____

George Christian
Plan II Honors
Supervising Professor

_____

Cesare Fracassi
Finance
Second Reader

ABSTRACT

Author: Hasan Syed

Title: Power to The People: How Blockchain Based Digital Identity Can Empower Disadvantaged Individuals

Supervising Professors: George Christian, Cesare Fracassi

Blockchain technology is thrown around as a fix for many logistical issues, including how societies keeps track of identity. 1.1 billion people currently lack any form of identity, and billions of people with identity find their personal data out of their control. Billions suffer when physical forms of identity are taken, destroyed, misplaced, or forged. The Equifax and Facebook-Cambridge Analytica hacks demonstrate the severe impacts of identity and data mismanagement. The European Migration Crisis exemplifies the drawbacks of immigration systems when physical identity forms are missing and the strenuous process of determining backgrounds and identity.

This thesis evaluates blockchain technology as a solution to the identity crisis. The thesis analyzes the specifics of the technology to see if it can function as an identity management system. It will then assess the viability of blockchain based digital identity projects. The paper will then apply the technology in hypothetical use cases and determine how blockchain architecture can empower individuals to reclaim control of their identity, especially in refugee and trafficking crises.

TABLE OF CONTENTS

Introduction

Blockchain technology is heralded as the fix for modern day issues in currencies, supply chains, healthcare records, voting, digital identity, and almost anything else. One use case, digital identity, promises that blockchain can transform identity into self-sovereign identity, where users have full control of their identity and data. Identity remains at the core of human interaction and trust – a verified, permanent, and digital version of identity could transform how individuals transact with one another. This paper will assess the viability of blockchain-based identity and evaluate potential applications for distressed societal groups, including refugees and trafficking victims.

Identity Crisis

An estimated 1.1 billion people worldwide lack documented identity.[1] This prevents many citizens from gaining access to healthcare, education, and employment amongst other things. A large portion of the world's unidentified citizens live without economic and social inclusion in society. Recent refugee crises in the Middle East, Europe, Africa and other parts of the world demonstrate the negative impacts stemming from lack of identification both within and across borders. The UN Sustainable Development Goal Target 16.9 seeks to provide legal identity for all, including free birth registrations by 2030.[2]

In the context of refugees, the lack of verifiable identity can pose serious threats to their livelihoods. The UN High Commissioner for Refugees (UNHCR) explains that "for a refugee,

[1] "1.1 Billion 'Invisible' People without ID Are Priority for New High Level Advisory Council on Identification for Development," Text/HTML, World Bank, 1, accessed March 26, 2019, http://www.worldbank.org/en/news/press-release/2017/10/12/11-billion-invisible-people-without-id-are-priority-for-new-high-level-advisory-council-on-identification-for-development.

[2] UN General Assembly, "United Nations Official Document, Transforming Our World: The 2030 Agenda for Sustainable Development," accessed March 26, 2019, http://www.un.org/ga/search/view_doc.asp?symbol=A/70/L.1&Lang=E.

the lack of identity documents may be far more than a source of inconvenience. In almost all countries an alien must be able to prove not only their identity but also that their presence in the country is lawful. In some countries aliens without appropriate documentation are subject to detention and sometimes even to summary expulsion. Such measures are particularly serious for a refugee, for whom they could also involve the risk of being returned to their country of origin. Even where the consequences of being without documentation are less drastic, the refugee, in order to benefit from treatment in accordance with internationally accepted standards, needs to be able to establish vis-à-vis government officials not only their identity but also their refugee character."[3]

Technology Overview

Blockchain Technology and Application to Digital Identity

Blockchain technology offers a potential solution to the global identity crisis by recording individuals with a digital identity tracked on a distributed ledger throughout a decentralized network. To assess the application of blockchain technology for digital identity, this paper will explain how blockchain technology works by overviewing key components such as: distributed ledger technology, smart contracts, permissioned blockchain and the use of private and public keys. This foundation can serve as framework for going forward in understanding the abilities and limitations of blockchain in identity projects.

Blockchain is an open, distributed ledger that can record transactions between two parties efficiently and in a verifiable and permanent way. The ledger itself can also be programmed to

[3] United Nations High Commissioner for Refugees, "Identity Documents for Refugees," UNHCR, accessed March 26, 2019, https://www.unhcr.org/excom/scip/3ae68cce4/identity-documents-refugees.html.

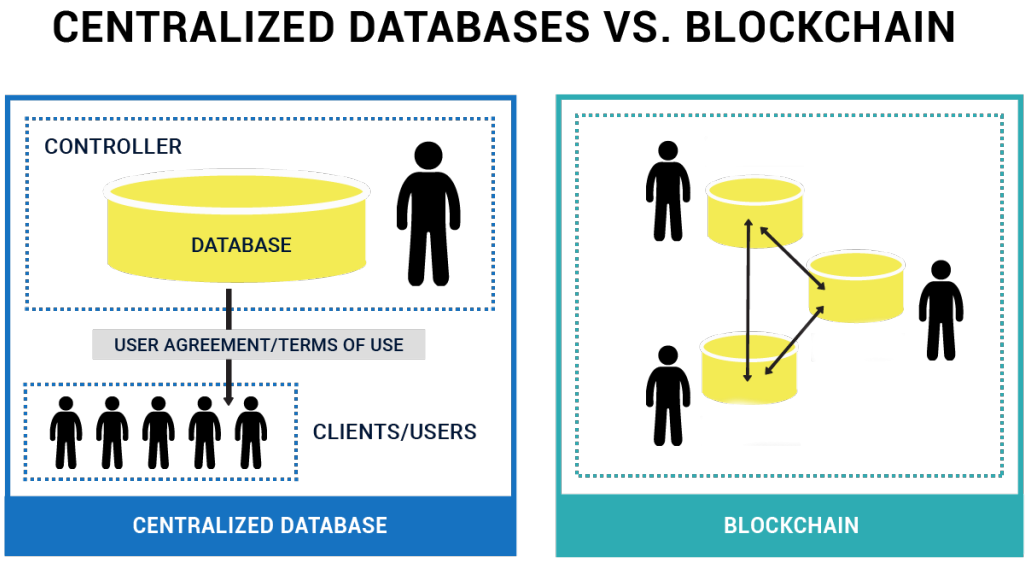
trigger transactions automatically.[4] Satoshi Nakamoto, an unknown identity, invented blockchain in 2008 as the technology to serve as a ledger for the cryptocurrency Bitcoin. Blockchain tracks assets or anything of value. It then groups those transactions into a block that must be verified by the blockchain network through consensus. Consensus, which will be discussed later, serves as the means to which the entire network verifies the block for it to then be added to the blockchain. This paper will now explore the major concepts of blockchain technology that will pertain to the application of blockchain in digital identity.

Distributed Ledger Technology

Blockchain is a type of distributed ledger technology (DLT). A distributed ledger distributes a database (a ledger) of transactions to all participants in a network (also called "peers" or "nodes"). There is no central administrator or centralized data storage.[5] For identity and security purposes, having a centralized database, such as that of a central government, allows for one entity to control the data and easily modify or delete it. Blockchain has no administrative privileges that allow for editing and deleting of data.

[4] Marco Iansiti and Karim R. Lakhani, "The Truth About Blockchain," *Harvard Business Review*, January 1, 2017, https://hbr.org/2017/01/the-truth-about-blockchain.
[5] "Blockchains (Continued) | Distributed Ledger Technology (DLT) | LFS171x Courseware | EdX."

The figure below depicts this key organizational difference.



(Figure from EDX Hyperledger)[6]

Network Architecture and Security

The ledger distributes and verifies itself across the network through peer to peer network architecture, meaning that nodes connect directly to each other rather than at a central server. For the purposes of security, especially with sensitive identity documents, peer to peer networks do not have a single point of attack - centralized networks do.

Another advantage, and possibly the most differentiable, of blockchain comes from the immutability of data. To verify a transaction, the network must achieve consensus through a

[6] "Blockchains (Continued) | Distributed Ledger Technology (DLT) | LFS171x Courseware | EdX," accessed March 26, 2019, https://courses.edx.org/courses/course-v1:LinuxFoundationX+LFS171x+3T2017/courseware/4bdba535373943059204 3585c7fbf044/bf7a3e04813b46e79773b5b55f339861/6?activate_block_id=block-v1%3ALinuxFoundationX%2BLFS171x%2B3T2017%2Btype%40html%2Bblock%400957d77a70354ae5beed429603a4da4a.

consensus algorithm. This process allows for the entire network to ensure the data remains the same across all nodes and prevents hacking. There are many different types of consensus algorithms, the bitcoin blockchain uses a proof-of-work algorithm, which relies on someone (a miner) from the network completing a complex mathematical problem that requires immense computing power. Imagine guessing millions of combinations for a lock to solve the problem. Once the problem is solved it can be verified by all other users on the network easily, like entering the right combination for a lock and seeing if it opens. This process requires a lot of energy and if a group of miners control over 50% of the network's computing power it can be susceptible to attack. If one group of miners gain access to the majority of the network, they can then choose which transactions get added to blocks and can even receive payments for transactions without adding them to the chain, leaving no trace of the transfer of money. This attack remains incredibly difficult to execute. For digital identity purposes, a Simplified Byzantine Fault Tolerance (SBFT) consensus algorithm provides a more secure, modified version of the proof-of-work algorithm. The Linux foundation provides an explanation of how this works:

> The basic idea involves a single validator who bundles proposed transactions and forms a new block. Note that, unlike the Bitcoin blockchain, the validator is a known party, given the permissioned nature of the ledger. Consensus is achieved as a result of a minimum number of *other nodes* in the network ratifying the new block. In order to be tolerant of a Byzantine fault, the number of nodes that must reach consensus is **2*f*+1** in a system containing **3*f*+1**nodes, where ***f*** is the number of faults in the system. For example, if we have 7 nodes in the system, then 5 of those nodes must agree if 2 of the nodes are acting in a faulty manner."[7]

[7] "Simplified Byzantine Fault Tolerance (SBFT) | Consensus Algorithms | LFS171x Courseware | EdX," accessed March 26, 2019, https://courses.edx.org/courses/course-v1:LinuxFoundationX+LFS171x+3T2017/courseware/4bdba535373943059204 3585c7fbf044/42a0909f1f6f4930a6501be2d72a5905/5?activate_block_id=block-v1%3ALinuxFoundationX%2BLFS171x%2B3T2017%2Btype%40vertical%2Bblock%40a17f832561fa4511ae4b933777175e69.

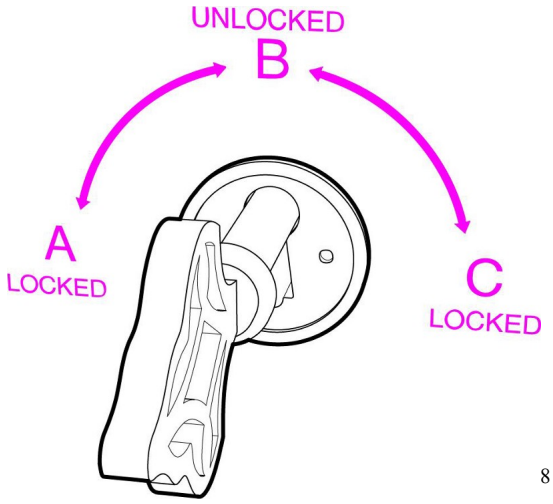
This concept will serve as the basis for a blockchain network used for digital identity tracking across governing and regularity bodies proposed later in this paper.

Types of Blockchains

As mentioned earlier, blockchains distribute a ledger to all nodes in a network. The network can remain public (permissionless), where anyone can join the network, or private (permissioned) where pre-verification of the parties must exist within the network. Public blockchains can work well for e-commerce. Any two parties can exchange value without requiring the need to know the identity of the other user, only the verification of the transaction remains important when transferring currency for an asset. With more sensitive data, such as digital identity documentation, a permissioned blockchain restricts only vetted parties in participating on the blockchain, allowing the information to remain verified, secure and confidential among specific participants.

Public Keys and Private Keys

In order for transactions of confidential data or identity to remain secure on a blockchain network, there must exist a public key and a private key. Take for example a normal password (private key) used to open an encrypted box. In symmetric cryptography, the user or anyone with the key (password) can open and close this box and access what's inside. Public key (asymmetric cryptography) works with having two keys. Vyronis explains this scenario with the analogy of a box with three states A (locked), B (unlocked) and C (locked). A public key can unlock the box by only turning from C to B and then back to A. The private key can turn the box lock from A to B to C.



[8]

In this situation, say a citizen fleeing their country trying to store claims to their identity in this "box", holds the private key. They can give out as many copies of public keys as they want to different parties, including their board that verifies their profession, or another with their identity details and so on. If one of these entities would like to reference a document or even deposit one into the box, they can use their public key to unlock the box from C to B, access the verified identity claim and then lock the box by turning only to position A. Now the individual with their private key is the only one that can access these private documents as the private key can only turn the lock from A to B and then locked back to C. Parties with a public key can deposit confidential information and trust that only the secure party with the private key, the citizen in this case, can only access it.

Now say the citizen needs to send identity verification claims to a third party, say an immigration service. They can use their private key to turn the lock to C, which the public key can lock and verify that these documents came from the individual as the lock encryption in

[8] Panayotis Vryonis, "Explaining Public-Key Cryptography to Non-Geeks," *Panayotis Vryonis* (blog), August 27, 2013, https://medium.com/@vrypan/explaining-public-key-cryptography-to-non-geeks-f0994b3c2d5.

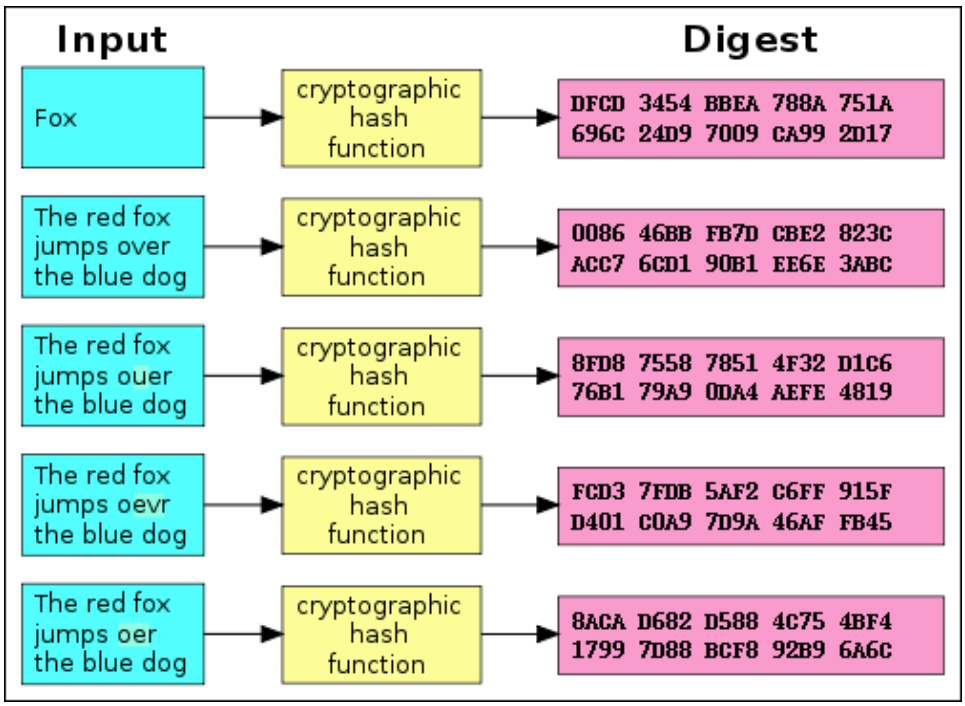
position C could have only been done with the private key – this demonstrates the citizen's digital signature.[9]

Cryptographic Hash Functions and Merkle Trees

Cryptography is the science of transmitting messages and transactions securely against third party adversaries. The objective of any transaction ensures the message is sent and received to and from the right parties while staying private and unaltered. Hashing is one cryptographic system that achieves these objectives by transforming a text of any arbitrary length into an almost irreversible fixed length string of numbers and letters.[10] Every time you input the same text, say "hello", the same hash is produced. Hashing exists as a one-way function, making it infeasible to decrypt the fixed length hashed text by trying to reverse the function back to the original "hello".

[9] Vryonis.
[10] Cesare Fracassi, "Intro to Cryptography FIN 294" (Spring 2019).

The image below depicts this process:[11]

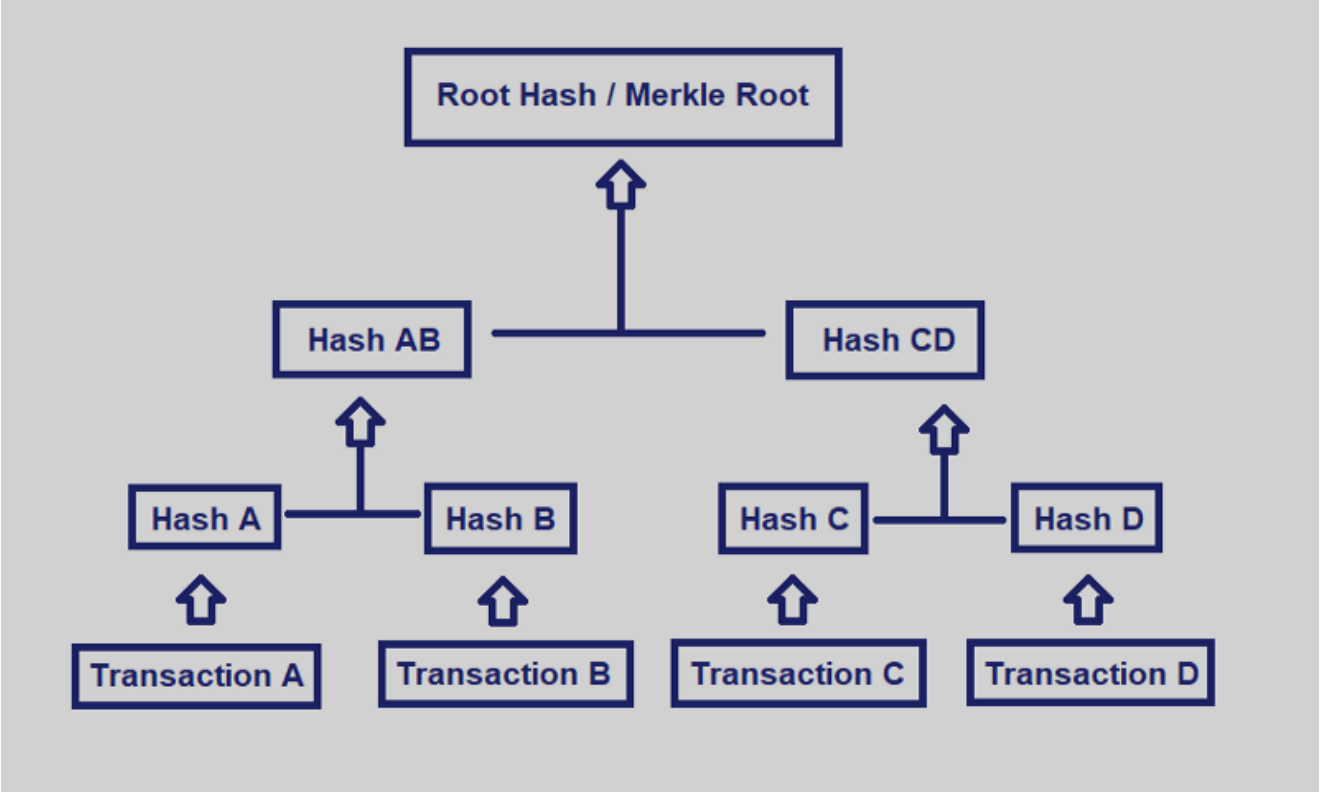


Notice how in the image above the slightest change in the word "over" to "ouer" completely transforms the hash output. The immutability of data on the blockchain is a result of hashing. Each block in a blockchain contains data and then a hash pointer, the address of the previous block along with a hash of the data inside the previous block.[12]

Each block contains thousands of transactions. Storing the data efficiently and quickly referencing a particular transaction occurs quickly thanks to the organization of the Merkle tree. A Merkle tree summarizes all the transactions in a block by producing a digital fingerprint of the

[11] "What Are MD5, SHA-1, and SHA-256 Hashes, and How Do I Check Them?," accessed March 31, 2019, https://www.howtogeek.com/67241/htg-explains-what-are-md5-sha-1-hashes-and-how-do-i-check-them/.
[12] "What Is Hashing? Under The Hood Of Blockchain - Blockgeeks," accessed March 31, 2019, https://blockgeeks.com/guides/what-is-hashing/.

entire set of transactions, thereby enabling a user to verify whether or not a transaction is included in a block.[13]



Each transaction has a transaction ID and the hash of each individual ID forms the leaf node as shown in the bottom layer of the diagram above. Hash AB and Hash CD are non-leaf nodes and contain hashes of the previous hashes in the layer below. At the top of tree lies the Root Hash which summarizes the data in the transactions and is the hash that is placed in the header of the block in the blockchain. The Merkle tree allows for a quick test to verify transactions in a block without having to check each individual transaction hash. Say John claims to have completed Transaction A (paying Stacy some amount of cryptocurrency), John would send the transaction ID and the hash above it (AB). The verifier already has the Root Hash so all that needs to be

[13] Shaan Ray, "Merkle Trees," Hacker Noon, December 15, 2017, https://hackernoon.com/merkle-trees-181cb4bc30b4.

done is hash the values on the particular branch of the tree that John's transaction A lies in to see if the same hash trail outputs to get the same Root. This process checks just the branch of the Merkle tree with the transaction without having to check every single transaction and the hash trails above it, making the process incredibly efficient and of relatively lower computing power.[14]

Encryption

Since hashing is a one way process and cannot be decrypted, it is not a form of encryption. Encrypted messages make sure that the message is transferred without being read or altered by anyone else.

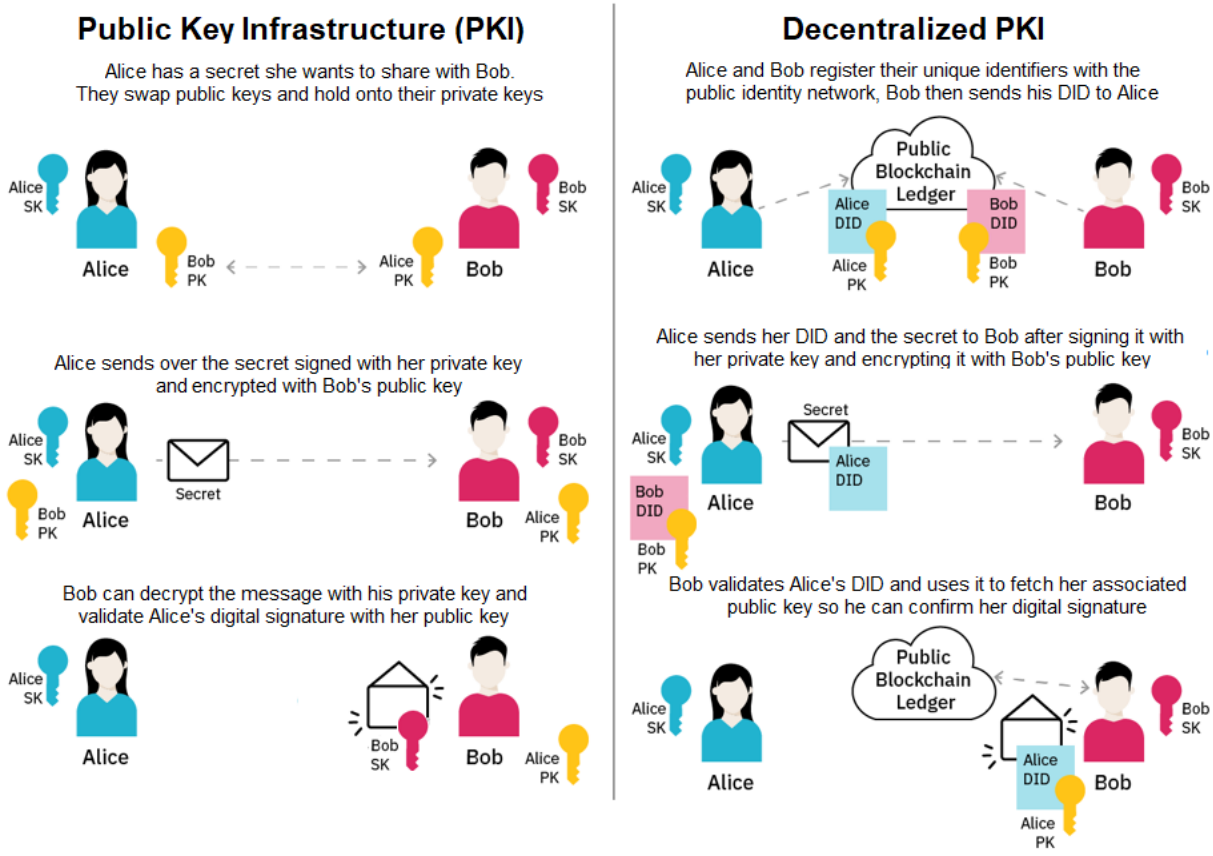
Symmetric key algorithms allow for the sender to send a message with a key that receiver can use to decipher the messages. Each receiver needs a secret key and it needs to be shared securely between both parties. Thus, symmetric key algorithms best work with two parties. Blockchain technology works with asymmetric key algorithms where only the receiver holds the key to decipher the message.

Asymmetrical cryptography uses public/private key pair to encrypt and decrypt messages and eliminates the need for the sending of the secure key back and forth and instead sends out numerous public keys to each receiver. To transfer data or a message, the receiver creates a private key and a public key, the public is made available to every sender via a public directory. The sender uses the public key to encrypt the message and sends the encrypted text (cipher text) to the receiver who can now decipher the text with their private key. Asymmetric encryption in

[14] "What's A Merkle Tree? Komodo's Guide To Understanding Merkle Trees," *Komodo* (blog), July 19, 2018, https://komodoplatform.com/whats-merkle-tree/.

blockchain technology allows for encryption across communications on an entire network as any sender can have a public key.

In the instance of digital identity on the blockchain, any entity (a person, organization or device) can create a unique decentralized identifier (DID) and write it to the public ledger. Now anyone trying to reference a DID can discover it from the public ledger and "acquire access to the associated public keys for verification purpose."[15]



[15] "Self-Sovereign Identity: Why Blockchain? - Blockchain Pulse: IBM Blockchain Blog," accessed March 31, 2019, https://www.ibm.com/blogs/blockchain/2018/06/self-sovereign-identity-why-blockchain/.

Smart Contracts

A smart contract is a computer protocol that facilitates the transfer of digital assets between parties under the agreed-upon stipulations or terms. It is similar to a traditional contract in most ways including definition of rules and penalties around the agreement except for the fact that it can also enforce the agreed-upon obligations automatically.[16]

Smart contracts self-execute, meaning they run as computer programs that execute predefined actions when certain conditions are met. Storing identification, certifications, and other valuable assets on a permissioned blockchain can allow for smart contracts to verify the identification and then issue appropriate authorizations without the need for a lawyer, notary or other third party. Employers and governments can setup smart contracts to automatically pay taxes upon wages paid out. This paper will later analyze possible use cases and implementation for smart contracts in varying self-sovereign identity use cases.

Hyperledger and Hyperledger Indy

Hyperledger Indy currently serves as one method for deploying digital identity and serves as the main medium for the possible solutions discussed in this paper. In many cases blockchain's popularity is known for its record keeping of cryptocurrencies. Hyperledger is a group of open source projects focused around cross-industry distributed ledger technologies. Hyperledger provides an alternative to the cryptocurrency-based blockchain model, and focuses on developing blockchain frameworks and modules to support global enterprise solutions.[17]

---

[16] "What Is a Smart Contract? - Definition from Techopedia," accessed April 1, 2019, https://www.techopedia.com/definition/32499/smart-contract.

[17] "Hyperledger Indy | Hyperledger Frameworks | LFS171x Courseware | EdX," accessed March 26, 2019, https://courses.edx.org/courses/course-v1:LinuxFoundationX+LFS171x+3T2017/courseware/fa54f0debd00468695b36d6ce87dc070/6a977492dec44c

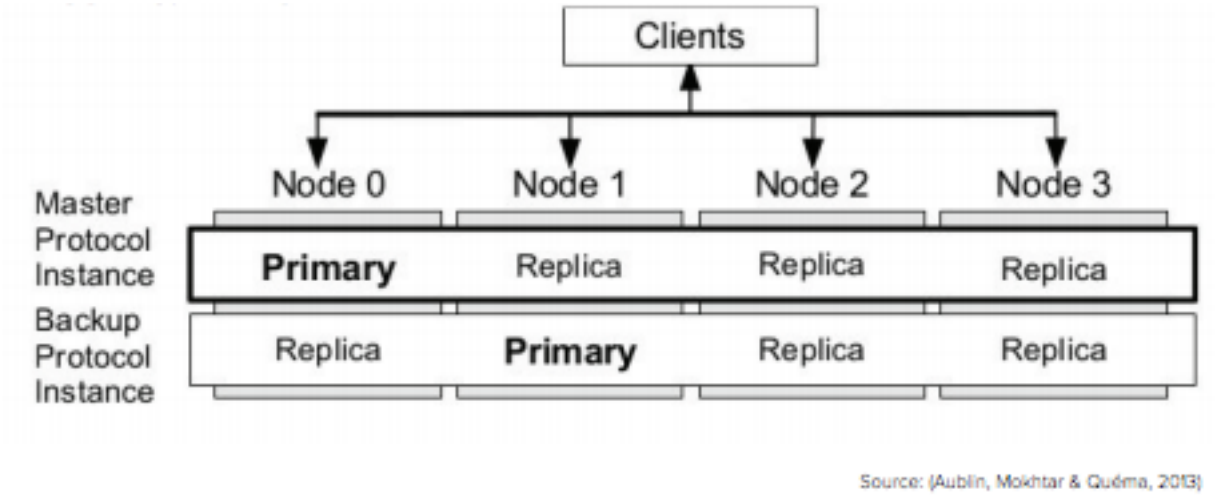
Currently, Hyperledger consists of 5 distributed ledger projects, one of which (Indy) focuses on digital identity on the blockchain.

Hyperledger Indy allows individuals to manage and control their digital identities. Rather than having entities store huge amounts of personal data of individuals, Hyperledger Indy allows businesses or other entities to store pointers to identity. Once the company verifies the other party's identity, it throws it away.[18] This identifies an individual and rather than writing private data to the ledger, it instead gets exchanged off a peer to peer private network encryption. This allows the identity holder to control their personal data rather than have it stored on a central server such as Equifax that can easily be breached. Validation on the ledger works through a modified version of the Byzantine Fault Tolerance consensus algorithm called Plenum. This differs slightly from the previously described SBFT consensus algorithm. Plenum protocol runs multiple instances of the same request across the network of one master and multiple backup instances. All instances carry out the requests but only the instance of the master is executed. The backups study the action of the master and make sure it remains consistent with the actions of all other instances. If not the master is considered malicious and replaced.

32a9e80c8a29372104/11?activate_block_id=block-v1%3ALinuxFoundationX%2BLFS171x%2B3T2017%2Btype%40vertical%2Bblock%40baad2d38202d4a9db52a26a9066af2a7.

[18] "Hyperledger Indy | Hyperledger Frameworks | LFS171x Courseware | EdX."

An overview is shown below.



(Plenum Protocol)[19]

Analysis of Current Projects

Some nations and organizations have begun processing identity digitally and even through blockchain. In Estonia, the government's development of electronic residency enables people from all around the world to digitally register themselves under the validity of the Estonian government. They can even start a business registered in Estonia. Canada announced testing blockchain technology for a known traveler identity for air travel use.[20] In Jordan, Syrian refugees can use a blockchain digital wallet for payment of goods.[21] India has registered 1.1

[19] Pierre-Louis Aublin, Sonia Ben Mokhtar, and Vivien Quema, "RBFT: Redundant Byzantine Fault Tolerance," in *2013 IEEE 33rd International Conference on Distributed Computing Systems* (2013 IEEE 33rd International Conference on Distributed Computing Systems (ICDCS), Philadelphia, PA, USA: IEEE, 2013), 297–306, https://doi.org/10.1109/ICDCS.2013.53.
[20] "Canada Tests Biometrics and Blockchain as Airports Worldwide Extend Biometric Use," *Biometric Technology Today* 2018, no. 2 (February 1, 2018): 11–12, https://doi.org/10.1016/S0969-4765(18)30026-2.
[21] "Inside the Jordan Refugee Camp That Runs on Blockchain - MIT Technology Review," accessed March 26, 2019, https://www.technologyreview.com/s/610806/inside-the-jordan-refugee-camp-that-runs-on-blockchain/.

billion people digitally through the Adhaar program.[22] Cities like Austin and others in the US have begun testing use cases for blockchain in tracking identification and vital records of homeless people.[23] Digital identity projects throughout the world can provide an understanding of the functional capabilities of blockchain identity tracking in the real world as well as obstacles. An analysis of these use cases can provide a better understanding of how to solve portions of the global digital identity crisis.

Estonia E-Residency

In December 2014, Estonia started issuing e-ID cards to e-Residents and became the first nation to open its digital borders to foreigners, through its e-Residency initiative. For the first time, a nation has enabled anyone anywhere in the world to have an international digital commercial life using a sovereign government-backed identity credential.[24] Although this does grant the right to entrance or citizenship, it does allow for a government authenticated digital identity, issuable to people around the world electronically. The Estonian government plans to have 10 million e-Residents by 2025, considerably more than the country's population of 1.3 million.[25] This program allows e-Residents to open bank accounts, buy and sell real estate or even start an EU registered business online.[26]

---

[22] ALAN GELB and ANNA DIOFASI METZ, "Identification Systems:: Innovations in Technology and ID Provision," in *Identification Revolution*, Can Digital ID Be Harnessed for Development? (Brookings Institution Press, 2018), 91–124, https://www.jstor.org/stable/10.7864/j.ctt21c4t40.8.

[23] "Austin Is Piloting Blockchain to Improve Homeless Services," *TechCrunch* (blog), accessed March 26, 2019, http://social.techcrunch.com/2018/04/14/austin-is-piloting-blockchain-to-improve-homeless-services/.

[24] Clare Sullivan and Eric Burger, "E-Residency and Blockchain," *Computer Law & Security Review* 33, no. 4 (August 1, 2017): 470–81, https://doi.org/10.1016/j.clsr.2017.03.016.

[25] e-estonia, *Estonian E-Residency's First Anniversary*, accessed March 26, 2019, https://www.youtube.com/watch?v=exyg1Eybcjw.

[26] "How to Start a Company in Estonia & EU," *E-Residency* (blog), accessed May 10, 2019, https://e-resident.gov.ee/start-a-company/.

Estonia grants e-Residency by having applicants scan their passport or national ID card online, which Estonia then conducts a background check on. Generally, digital identity in other nations require multiple forms of identification, with original copies, not scans and then an in person meeting to verify the photo. Estonia's government effectively makes the assumption that other countries national ID standards have already done this and thus assumes validity based on a passport or national ID card. Applicants can then pick up their smart card just by presenting the same piece of documentation. Fingerprints are taken upon collection of the card to serve as a biometric authentication method for identity.[27] Issues arise as "an easily obtainable transnational digital identity that enables unreported and unmonitored trade and commerce is the ideal vehicle for fraud, tax avoidance and money laundering. Money laundered in this way can then be used to fund crime and terrorist activity domestically and internationally."[28] This process presents many obstacles for applying this style of identity registration to unidentified people as it poses too many security threats – a revised version must address the authenticity concerns.

In 2015, Estonia partnered with Bitnation, self-proclaimed as "the world's first Decentralized Borderless Voluntary Nation", to allow "e-Residents, regardless of where they live or do business, to notarize their marriages, birth certificates, business contracts, and much more on the blockchain."[29] Government systems can take passports, bills and supporting documentation to authenticate identities directly from the passport office, utility company or any entity through the distributed ledger where each entity holds copies. Such authentication could allow for the use of these administered identities across transnational boundaries if other

[27] Sullivan and Burger, "E-Residency and Blockchain."
[28] Sullivan and Burger.
[29] e-estonia, *Estonian E-Residency's First Anniversary*.

countries uphold Estonia's validity. Currently Estonia, Belgium, Portugal, Lithuania, and Finland mutually recognize e-ID's.[30]

Legal complications abound when digital identity transition goes from verification by a central government to a distributed ledger, such as Estonia's project with Bitnation. In the journal of *Computer, Law & Security Review*, Eric Burger explains "Bitnation is not a sovereign nation and as of the time of this writing has no legitimacy in law. That is, none of the transactions registered by Bitnation have any legal standing, unless also recognized by a real sovereign nation. For example, no one will recognize a 'wedding' registered at Bitnation that is not also recognized by some other state. Note that this occurs between real states as well. For example, a marriage between two men in the Commonwealth of Massachusetts is recognized in the United States but will not be recognized in the Russian Federation. The difference is, as of now, no national will recognize a marriage registered by Bitnation."[31] The Estonian government, in their partnership with Bitnation, recognizes notary services such as marriages registered on with Bitnation.[32] Other governments have yet to follow suit. Estonia's use of e-residency and blockchain backed digital identity can pave the way for other governments to begin recognizing decentralized networks as valid authenticators.

Zug Identity Project with uPort

On November 15, 2017, the first digital Zug ID officially registered on the Ethereum blockchain. The Swiss city of Zug embarked on a digital identity project to register citizenship through blockchain technology by using the self-sovereign identity platform, uPort. uPort runs

[30] Sullivan and Burger, "E-Residency and Blockchain."
[31] Sullivan and Burger.
[32] "Bitnation and Estonian Government Start Spreading Sovereign Jurisdiction on the Blockchain," International Business Times UK, November 28, 2015, https://www.ibtimes.co.uk/bitnation-estonian-government-start-spreading-sovereign-jurisdiction-blockchain-1530923.

off the Ethereum network and appears to end users as an app where they can encrypt their personal information and receive an ID which is linked to a cryptographic address on the Ethereum blockchain. Once the information is verified, users can interact with the digital services of the City of Zug.[33]

Citizens of Zug download the uPort mobile application and create a uPort ID, which they then use to register on the Zug web portal with their name, ID number, and date of birth. This request to register is cryptographically signed with their private key and sent to the city. Now the citizen has 14 days to go in person to the city clerk and verify their identity by providing their ID. The city of Zug can log on to their own identity on the Ethereum network as a "verified identity" and sign off on the citizen's attestation request. The ID verification remains cryptographically signed and visible on the blockchain; however, the actual attestation remains off-chain to prevent others from knowing a citizen's date of birth or passport information. The attestations remain managed by the citizen themselves, the data does not get stored on a central silo as it would say for a bank network or even Gmail. The control of the attestations by the individual is the basis for self-sovereign identity.[34] uPort seeks to streamline and secure the process of verifying an identity, referred to as Know Your Customer (KYC).

Data Security

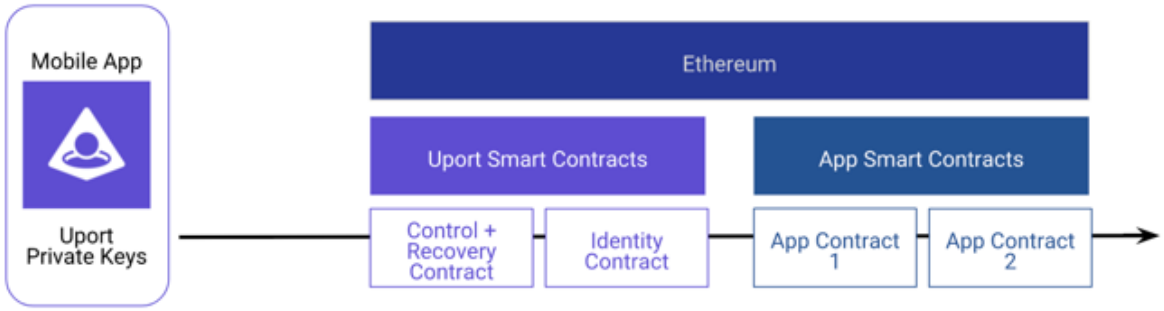
Advantages of the uPort system include the password-less nature of the interface. When the user wants to engage with another application all they need to do is scan a quick response (QR) code. Traditionally users have to sign on to other platforms by creating an account or using an existing Facebook or Google account to setup an identity to interact with another application.

---

[33] "UPort Announces Zug Digital Ethereum ID Pilot," ETHNews.com, accessed March 26, 2019, https://www.ethnews.com/uport-announces-zug-digital-ethereum-id-pilot.

[34] Linum Labs, *ConsenSys and UPort: Powering Decentralized Identity*, accessed March 26, 2019, https://www.youtube.com/watch?v=VXAZdBtN3N0.

This allows for the user to have control over their data. Applications that the identity engages do not store data on their end as the account remains managed by the uPort identity. Private keys are kept safe by being stored out of the uPort application and are kept on the phone itself in the same enclave where fingerprint and facial recognition data is stored.[35] Zug has began using uPort in this manner when partnering with AirBie, a crypto integrated bike sharing service. AirBie can "verify that users are able to not only verify that the individuals accessing their bikes are relatively trustworthy individuals ("Zug residents") but also can return data control back to the individuals."[36]



(Figure taken from uPort)[37]

Transparent and Decentralized Voting

Since the launch of uPort managed digital identity in Zug, over 300 citizens registered their citizenship digitally. On June 25, 2018, 72 electronically registered citizens of the city piloted the first e-vote on the uPort platform. This proof of concept for decentralized voting

[35] Linum Labs.
[36] Alice Nawfal, "Zug Residents Can Now Ride E-Bikes Using Their UPort-Powered Zug Digital IDs," *Medium* (blog), November 14, 2018, https://medium.com/uport/zug-residents-can-now-ride-e-bikes-using-their-uport-powered-zug-digital-ids-7ed31ac9d621.
[37] "UPort Controller Contracts," accessed March 26, 2019, https://developer.uport.meundefined/overview/index.

exhibited the security advantages over a traditional centralized system. The Lucerne University of Applied Sciences and Arts evaluates the advantages of the Zug eVote trial by finding:

> With blockchain supported effective identity management, it is infeasible for hackers to impersonate voters. Secondly, techniques like digital signatures protect the integrity of the data, meaning votes cannot be tampered with in transit. Thirdly, the blockchain is immutable – once a vote has been recorded, it cannot be removed or altered. As the data is stored across multiple nodes, even if one or several nodes are hacked, the voting data cannot be destroyed by hackers. As long as there are enough nodes, it is almost impossible for the whole system to be compromised.[38]

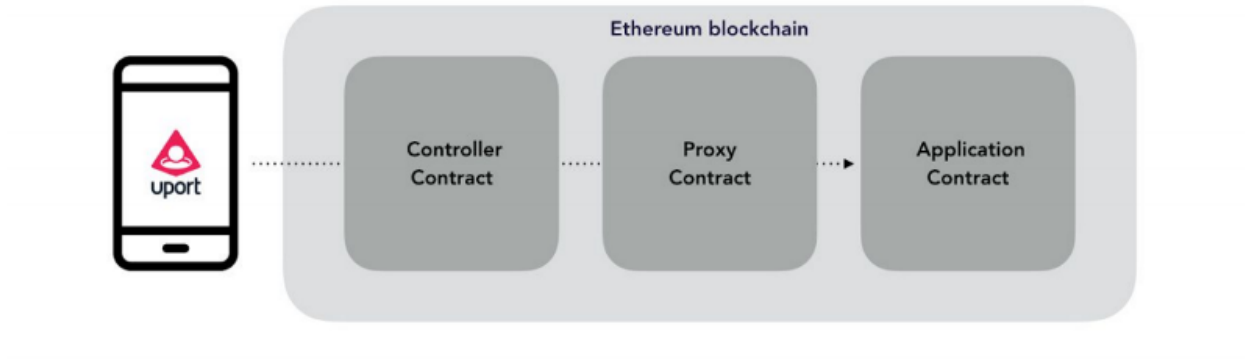
Following the pilot vote the city of Zug concluded that "this proof of concept was a success and is a significant milestone that demonstrates blockchain based e-voting systems work." [39]

Loss of Identity

In traditional public key cryptography systems, public keys represent identities. Identity ownership is determined by possession of the private key that controls the public key.[40] If the user's phone is stolen, lost or even upgraded then identity is lost too, which would hinder any large scale adaptation of the technology by cities, countries and other users alike. In order to create a recovery method for lost private keys, uPort deployed three smart contracts for each new identity created. The creation of Proxy contract allows for persistent identity as its address is the identifier of the identity.[41] The Proxy contract allows a certain address to interact with the blockchain through itself. The Proxy contract is the avenue through which users interact with the rest of the Ethereum world. This allows a user to continue interacting with other smart contracts

[38] Lucerne University of Applied Sciences and Arts, "Evaluation of the Blockchain Vote in the City of Zug," November 30, 2018, 6.
[39] Lucerne University of Applied Sciences and Arts.
[40] Pelle Braendgaard, "What Is a UPort Identity?," *UPort* (blog), February 27, 2017, https://medium.com/uport/what-is-a-uport-identity-b790b065809c.
[41] Nate Rush, "Making the UPort Smart Contracts Smarter," *UPort* (blog), August 14, 2017, https://medium.com/uport/making-the-uport-smart-contracts-smarter-e1798d8c1cf9.

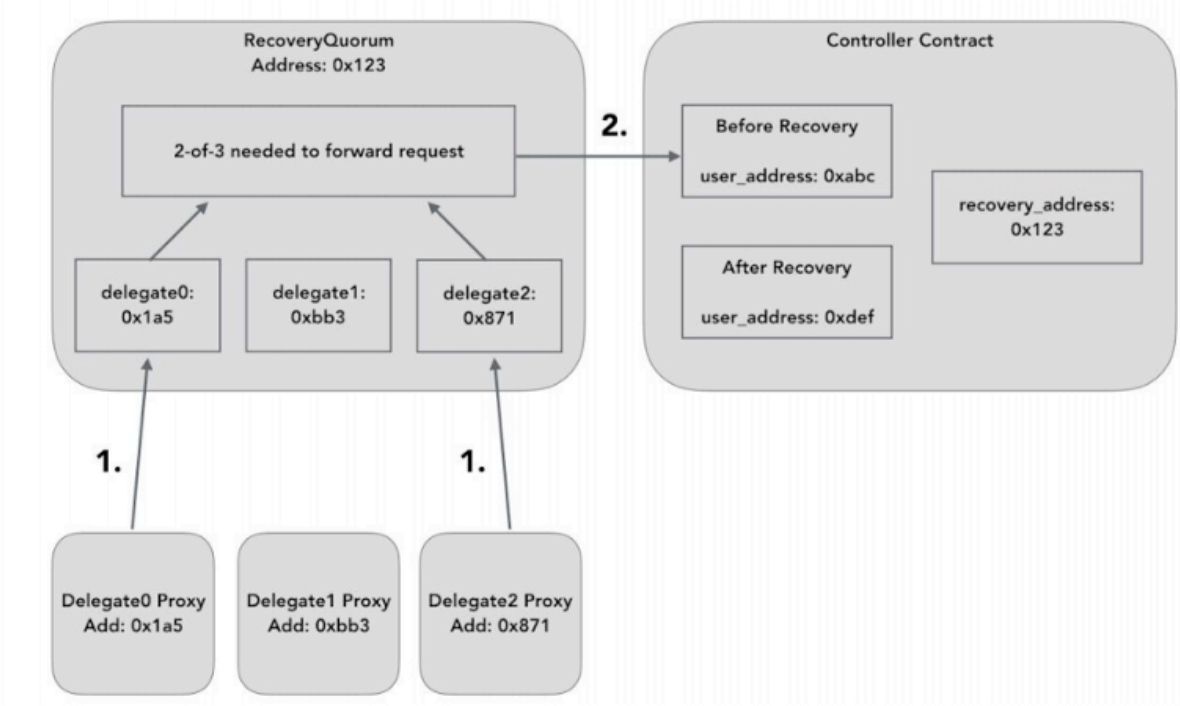
from a single address, even in the case of key loss.[42] The figure below depicts how the smart contracts interact with each other.



(Figure taken from uPort)[43]

The controller contract controls access to the proxy through the private key on the phone. If the phone goes missing, then the RecoverableController serves as a contract that allows users to recover their controller contract through either seed recovery from a secret backup key of 12-24 words the user holds or through a social network through uPort's RecoveryQuorum. The RecoveryQuorum asks users to assign other trusted uPort users (family or close friends perhaps) and asks them to vote to restore a user's Proxy contract. The network of trusted individuals can vote to restore the lost Proxy to the rightful owner as demonstrated in the following figure. This solution remains an Ethereum specific solution and does not work on other blockchains, limiting uPort's scope.

[42] Rush.
[43] Dr Christian Lundkvist et al., "UPORT: A PLATFORM FOR SELF-SOVEREIGN IDENTITY," n.d., 17.



(Figure taken from uPort)[44]

Drawbacks

Cost

Cost remains a major obstacle in the wide scale onboarding of uPort identities as each identity creation costs 2.4 million gas per (gas refers to the price paid for a transaction to occur on the Ethereum blockchain. This is the incentive for miners to validate transactions as they receive this payment). At the average conversion rate in March 2019 this cost would amount to approximately $30. The problem arises when new users have to buy Ether and interact with the Ethereum public chain, a complicated process for those unfamiliar with the interface.

In late 2018, uPort rolled out their newest update of the platform to try and solve this obstacle with a brand new architecture on a newly proposed Ethereum Standard: ERC1056

[44] Lundkvist et al.

Lightweight Identity which would push for the adoption of a standard for Ethereum Wallets.[45] This new proposal limits Blockchain interaction by creating an Ethereum key pair for identity, meaning initially no transaction takes place and an Ethereum address (last 20 bytes of the hash of the public key) is issued. Since the creation of the key pair does not require a transaction on the Ethereum blockchain, users do not have to pay for registering. uPort claims "the process is so rapid and seamless that millions of identities could be created in a single day, even without Ethereum supporting Proof of Stake or Sharding. This means we can finally support very large-scale applications, such as national identity projects."[46]

Security

The uPort identity allows for certain information about the user to be public such as one's name and image. This can be seen as the Ethereum equivalent of a Facebook profile. The uPort Registry is a "single smart contract shared by uPort identities that provides the infrastructure required for off-chain data sharing and verification of identity."[47] As mentioned earlier, not all transactions need to take place on the public blockchain as this would require Ethereum costs for processing but also ensure that certain private information such as a passport number is not being stored on a public blockchain. Off-chain transactions occur off the blockchain but users can still verify identity claims by querying the uPort Registry. If a user wants to transact privately and sign data off chain with their private key, they can do this by using the uPort Registry by searching a public key and assign signing permission.

[45] "ERC: Lightweight Identity · Issue #1056 · Ethereum/EIPs," GitHub, accessed March 26, 2019, https://github.com/ethereum/EIPs/issues/1056.
[46] Braendgaard, "What Is a UPort Identity?"
[47] Braendgaard.

The issue lies in the fact that the registry centralizes identifiers. Although the identity attributes remain encrypted, the public registry makes it possible for metadata on relationships between identity providers and parties can leak.[48]

Key Recovery Issues

The recovery protocol for uPort allows for a trusted network to help restore a user's uPort identity. Dunphy argues that this can pose as a major security threat as "the trustees themselves could be one vector of attack since their own uPortIDs are openly linked to the user's uPortID; this transparency provides opportunities for collusion against a specific uPort user. If an attacker can compromise a uPort application and replace trustees unnoticed via the controller, the uPortID is compromised permanently."[49]

Civic

Another self-sovereign identity project similar to uPort is Civic, which created the Civic Secure Identity Platform on their Civic App. The clients upload their personal identity information (PII) to the app which then verifies their identity, allowing them to become a Civic user. The Civic App stored the user's data on the phone using encryption and biometric locks (such as fingerprint ID).[50] The use of biometrics eliminates the need for usernames and passwords, which can be hacked. Civic identity partners (third parties using the Civic app for login or KYC) can request user information through QR codes scanned by the user on the app.

---

[48] Paul Dunphy and Fabien A. P. Petitcolas, "A First Look at Identity Management Schemes on the Blockchain," *ArXiv:1801.03294 [Cs]*, January 10, 2018, http://arxiv.org/abs/1801.03294.
[49] Dunphy and Petitcolas.
[50] Civic Technologies, "Civic Token Sale WhitePaper," accessed March 26, 2019, https://tokensale.civic.com/CivicTokenSaleWhitePaper.pdf.

Users have full control over the information being requested and can choose to approve the request.[51]

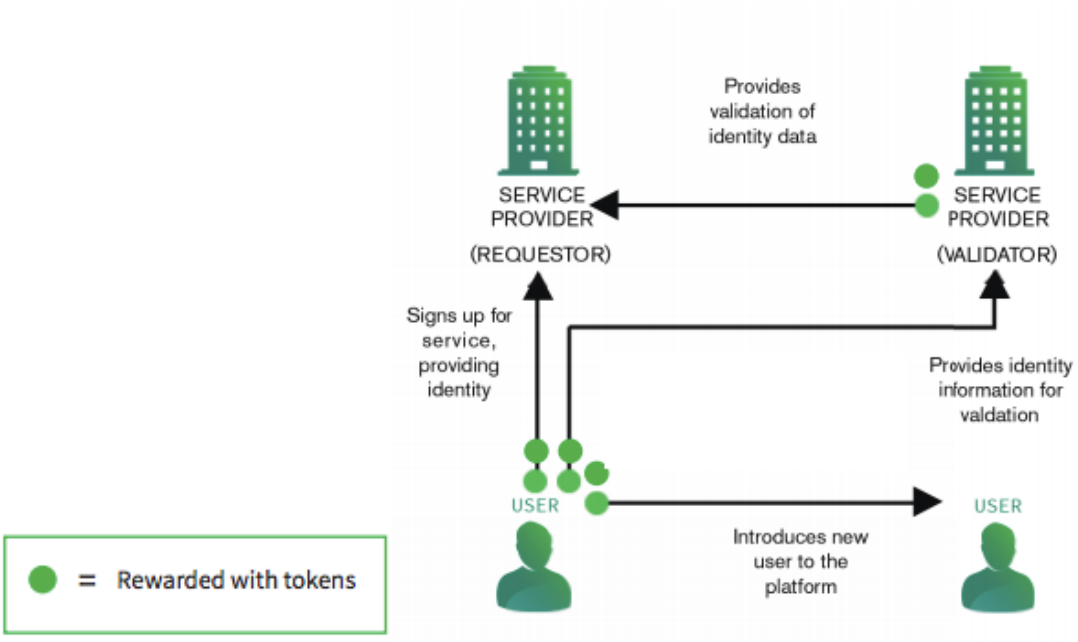
Civic Token Sales

An Initial Coin Offering shares some similarities to an Initial Public Offering for stocks on the market in the sense that both allow the respective entity to raise funds. In an IPO, a company "goes public" by opening up ownership to the public market, allowing for individuals to purchase equity in their company in exchange for funding. ICO's serve as a means for anyone creating a token or cryptocurrency to raise money to build or expand their project. It works by following a few steps. Initially the concept for the currency and system is introduced in a white paper that details how it would work. The white paper explains the value add of the project and shows how the currency does something necessary that has not been done before. Then comes the ICO where people are asked to purchase the token. The key difference between an ICO and IPO lies in the fact that ICO's do not forego any ownership. Investors purchase tokens with the expectation that the success of the currency will increase circulation and appreciate the token's value.

In June 2017, Civic had an initial coin offering where it sold $33 million in Civic tokens (CVC). Civic issued 1 billion total tokens of which it retained 33%, while 33% was allocated for distribution to incentivize participation in the ecosystem. Another third of the tokens were sold for the $33 million in the token sale and the last 1% covered the costs of the token sale. CVC is an Ethereum ERC20 (Ethereum Request for Comment 20), which means the token follows the technical standards required for smart contracts on the Ethereum blockchain.

[51] Civic Technologies.

Civic's token allows for the ecosystem to function by having validators receive CVCs when participants utilize their attestations to prove identities.[52] Users then receive CVCs for utilizing the system when they provide data. The use of a dedicated Civic token as opposed to an existing cryptocurrency such as Ethereum is called into question. Civic argues that a dedicated token allows for retention of a single uniform method of settlement across jurisdictions.[53] The nature of a token solely for identity services "provides stability and shields the Ecosystem from extraneous considerations that can make other cryptocurrencies volatile."[54] Civic also argues that the use of a token creates an ecosystem with an incentive structure for users and providers to validate identity as shown below.



(Figure taken from Civic white paper)[55]

[52] "Civic Identity Verification Crowdsale," accessed March 28, 2019, https://tokensale.civic.com/.
[53] Civic Technologies, "Civic Token Sale WhitePaper."
[54] Civic Technologies.
[55] Civic Technologies.

Verification Process

A major difference between the Civic platform and uPort's lies in the data verification process for identities. Civic claims "The Civic mobile app enables your users to scan and verify their identity documents so you can satisfy your company's KYC requirements.[56] Leverage trusted 3rd parties in the Identity.com Marketplace to validate personal information with blockchain attestations and store everything locally on the user's mobile device."[57]

The verification process forces users to pass a liveness test and a selfie comparison with their ID. The documentation also goes through optical character recognition to ensure the authenticity of the document. Checks in the United States abide standards such as the Customer Identification Program, which consists of name matching against lists and determining a customer's potential risk for money laundering, identity theft, and terrorism financing as it stacks against similar customer profiles."[58] Trustworthy validators (governments, financial institutions) can approve users' records through blockchain and store a hashed version of their PII as an attestation. Service providers can then pay the validators for attestations, pending user approval. Validators set the price for attestations. The smart contract will also deliver a portion of the paid CVC to the user to encourage participation in the Civic ecosystem.[59]

[56] "Anonymous Age Checks," Civic Technologies, Inc., accessed March 26, 2019, https://www.civic.com/solutions/vending-machines/.
[57] Civic Technologies, "Civic Token Sale WhitePaper."
[58] "Civic Decentralized Reusable KYC Services - Blockchain-Powered," Civic Technologies, Inc., accessed March 28, 2019, https://www.civic.com/solutions/kyc-services/.
[59] Civic Technologies, "Civic Token Sale WhitePaper."

(Figure taken from Civic)[60]

Civic finds that the cost of trying to verify identity ranges $15-20 for banks. This process generally remains the same for every bank and yet each bank runs their own KYC. A Thompson Reuters survey of 800 banks and their corporate customers found that the average bank spends $60 million on KYC compliance each year, and 89% of the customers reported a negative KYC

[60] "Civic Decentralized Reusable KYC Services - Blockchain-Powered."

experience, leading to 13% even changing their financial institution as a result.[61] 10 % of the world's financial institutions spend at least $100 million on KYC and banks take an average of 24 days to complete their customer onboarding process.[62] Civic argues these costs make their way to the customer eventually. Through Civic's token and ecosystem service providers can reuse KYC and limit that repeated cost of $15-20 by having service providers pay a small fee each time they interact with a validator for a verification. The likelihood of service providers making this switch depends entirely on the scale of the Civic IDV market and the size of the customer base. This process also depends heavily on the credibility of the validator. Reusable KYC relies on a marketplace where a previous service provider that paid for an identity verification then has the option to act as a validator and charge CVC when another service provider requests verification of the attestation of a user. The new service provider receives information that allows it to locate and view the past blockchain transaction where the attestation took place and can decide to purchase the attestation. They can pay the previous service provider in CVC which enters into a smart contract that can release the CVC upon the user approving the data share.

Advantages of Decentralized Data Source

Since the actual PII remains stored on a user's phone, a data breach would require an attack, person by person, as opposed to a centralized data breach. On a decentralized ecosystem such as that of Civic, each transaction would need actual proof of ownership as opposed to a simple data point such as a credit card number. Civic explains that "credit card details have black market value

[61] "Thomson Reuters 2016 Know Your Customer Surveys Reveal Escalating Costs and Complexity," accessed March 29, 2019, https://www.thomsonreuters.com/en/press-releases/2016/may/thomson-reuters-2016-know-your-customer-surveys.html.
[62] "Council Post: Know Your Customer (KYC) Will Be A Great Thing When It Works," accessed March 31, 2019, https://www.forbes.com/sites/forbestechcouncil/2018/07/10/know-your-customer-kyc-will-be-a-great-thing-when-it-works/#110a4ac78dbb.

because transactions can take place simply with knowledge of the data. Once a credit card number has to be presented with blockchain based proof the user indeed owns that number, the value of simply having those details progressively deteriorates with the adaption of the Ecosystem."[63]

Drawbacks

The ecosystem Civic is attempting to create consists of three parties, users, businesses and validators. To tap into the benefits Civic can offer, the platform needs to scale to a size where there lies an incentive for each of those three groups to use the platform. This becomes difficult as the sequencing must happen at the same time. If users download Civic but very few businesses utilize the application then the ecosystem fails; the same applies for validators if there are not enough transactions occurring to mine.

A major issue preventing the adoption of Civic and CVC lies in the illiquidity of the token. CVC is one of 1,600 tokens currently being traded on exchanges. With the sheer amount of tokens in circulation it becomes difficult for tokens with very few transactions in comparison to Ethereum or Bitcoin to gain value as utilization remains low. For many businesses or users, transacting in CVC just becomes another obstacle as fiat or Ethereum must be converted to interact with the platform. Thus, there is little incentive to hold onto to CVC in a wallet as there is no use for it beyond the ecosystem unlike Ethereum or Bitcoin.

Large scale adoption of the Civic secure identity platform could allow for individuals all around the world to take control of personal data and have accessible, mobile forms of documentation. The challenges in this solution ultimately lie in the difficulty in adopting such a disruptive technology.

[63] Civic Technologies, "Civic Token Sale WhitePaper."

Sovrin

In 2015, a startup named Evernym invested in the potential for blockchain technology to solve the root-of-trust problem for self-sovereign identity. Evernym began designing a new blockchain called Sovrin (taking the name from 'self-sovereign identity') to meet this need. On September 29, 2016, the Sovrin Foundation was announced in London. It is now an international non-profit foundation with a board of twelve trustees plus a Technical Governance Board. In early 2017 the Sovrin Foundation transferred the open source code base—originally contributed by Evernym—to the Linux Foundation to become the Hyperledger Indy project.[64]

Sovrin is an open sourced decentralized identity network built on permissioned distributed ledger technology.[65] Sovrin is public and open to all users, but only trusted institutions such as governments or banks can serve as the validators on the network. Sovrin argues that for identity to truly be universal and self-sovereign the platform must operate as a global public utility, similar to the Internet and Web. Open protocols, open standards, open source software along with open governance ensure that no one owns the technology and anyone can access and improve the utility. Sovrin believes that Bitcoin and Ethereum networks were not engineered for decentralized identity as the chief objective, thus this new public blockchain can better achieve these goals.

Governance

The trustees of the Sovrin Foundation established the Sovrin Governance Framework. This feature distinguishes Sovrin from other self-sovereign identity projects as it incorporates a degree of centralization to the ecosystem. The governance framework enables certain approved

[64] Sovrin Identity for All, "Sovrin™: A Protocol and Token for SelfSovereign Identity and Decentralized Trust," January 2018, https://sovrin.org/wp-content/uploads/2018/03/Sovrin-Protocol-and-Token-White-Paper.pdf.
[65] Dunphy and Petitcolas, "A First Look at Identity Management Schemes on the Blockchain."

institutions by the Sovrin Trust to serve as validators, which takes away from the fully decentralized, trustless nature of blockchain. Sovrin's governance structure allows for decisions on how code is architected, run and operated. The platform is built by an open source community and the governance structure allows for participators to decide which standards to adopt. This process is not too different from how governance in permissionless blockchains occur, where developers propose new standards and miners choose whether to implement them, enabling their adoption. When stewards propose changes on the Sovrin network, no single entity can force the adoption of the changes, consensus among the stewards democratically allows for agreed changes.

The Sovrin Governance Framework is the legal foundation and constitution of the Sovrin Network.[66] Anyone can apply to join the governing network. Organizations can apply to become stewards on the network as well on the governing framework. The foundation has laid out three legal agreements and six Controlled Documents on policies on governance in the network that participators must adhere to. The legal agreements are:

1. The Sovrin Steward Agreement between the Sovrin Foundation and a Sovrin steward.
2. The Transaction Author Agreement between the Sovrin Foundation and any person or organization initiating a write transaction to the Sovrin Ledger.
3. The Transaction Endorser Agreement between the Sovrin Foundation and any organization requiring permissioned write access to the Sovrin Ledger.[67]

Identity holds immense value and sensitivity; the legal framework allows for a system of accountability among everyone interacting in the ecosystem.

[66] Sovrin Identity for All, "Sovrin-Governance-Framework-V2-Master-Document-V1.Pdf," 2019, https://sovrin.org/wp-content/uploads/2019/03/Sovrin-Governance-Framework-V2-Master-Document-V1.pdf.
[67] "Sovrin Governance Framework," *Sovrin* (blog), accessed April 7, 2019, https://sovrin.org/library/sovrin-governance-framework/.

The first 24 stewards on the Sovrin Network include 11 countries, eight financial institutions, two law firms, one university and two NGOs.[68] Sovrin's architecture creates a system where no single entity controls or owns Sovrin, not even the Foundation. The governance structure maintains Sovrin's status as an open source model, ensuring its function as a public utility just like the internet.[69]

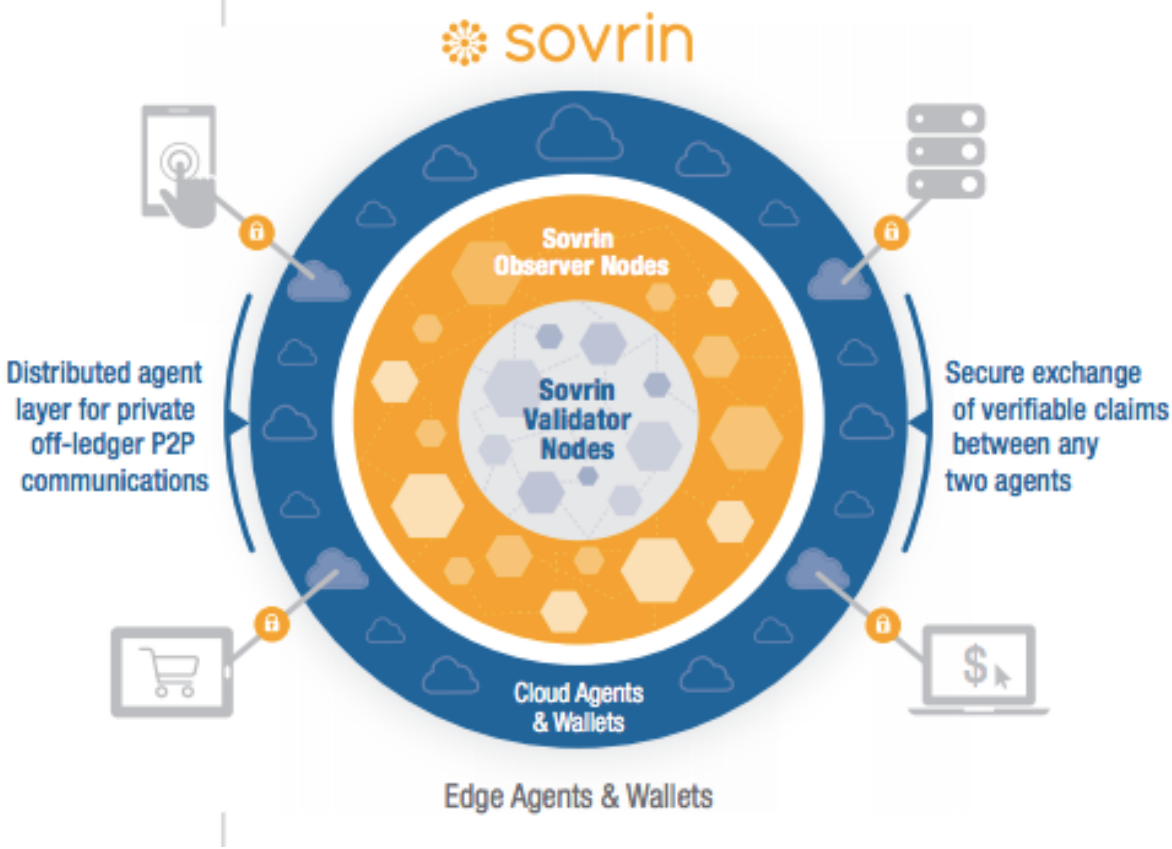
Performance

Sovrin allows for a user to generate as many identifiers as needed to preserve identity for privacy purposes. The advantage here is true privacy and anonymity. For example Bitcoin may conceal your real world identity but the same digital identifier is used for each anonymous transaction so a user's transactions can be triangulated. The Sovrin model operates under the assumption that transacting anything on a public blockchain is in a hostile environment.[70] Each time a user on the Sovrin network needs to transact or relate to, they receive a new identifier.

To sustain the billions if not trillions of decentralized identifiers created for global public utility, Sovrin has created a solution for addressing lag in the blockchain network. Typically, consensus protocols in Bitcoin, Ethereum and other networks are limited in scale as every node on the network must process every transaction and maintain a copy of the entire state. This lag can drastically increase the larger the network grows. The Sovrin Network addresses this by creating two rings of nodes. Validator nodes to accept and write transactions and then a much larger amount

[68] Sovrin Identity for All, "Sovrin™: A Protocol and Token for SelfSovereign Identity and Decentralized Trust."
[69] "Sovrin Governance Framework."
[70] Jamie Burke, "WHY WE ARE BACKING EVERNYM & THE SOVRIN FOUNDATION," *Outlier Ventures* (blog), October 22, 2017, https://medium.com/outlier-ventures-io/why-we-are-backing-evernym-the-sovrin-foundation-1822d2804991.

of observer nodes that run read only copies of the blockchain to process read requests. The figure below depicts the setup of the Sovrin Network's architecture.[71]



Token

The Sovrin token aims to address issues prevalent in the current KYC approaches. KYC processes typically occur only for high value credentials such as mortgages, background checks and so on. Low value credentials such as social network verifications or peer endorsements do not have the same or any KYC processes. The Sovrin token allows for a KYC market for lower value credentials as the verification credential for an individual already exists and verifiers can pay a

[71] Sovrin Identity for All, "Sovrin™: A Protocol and Token for SelfSovereign Identity and Decentralized Trust."

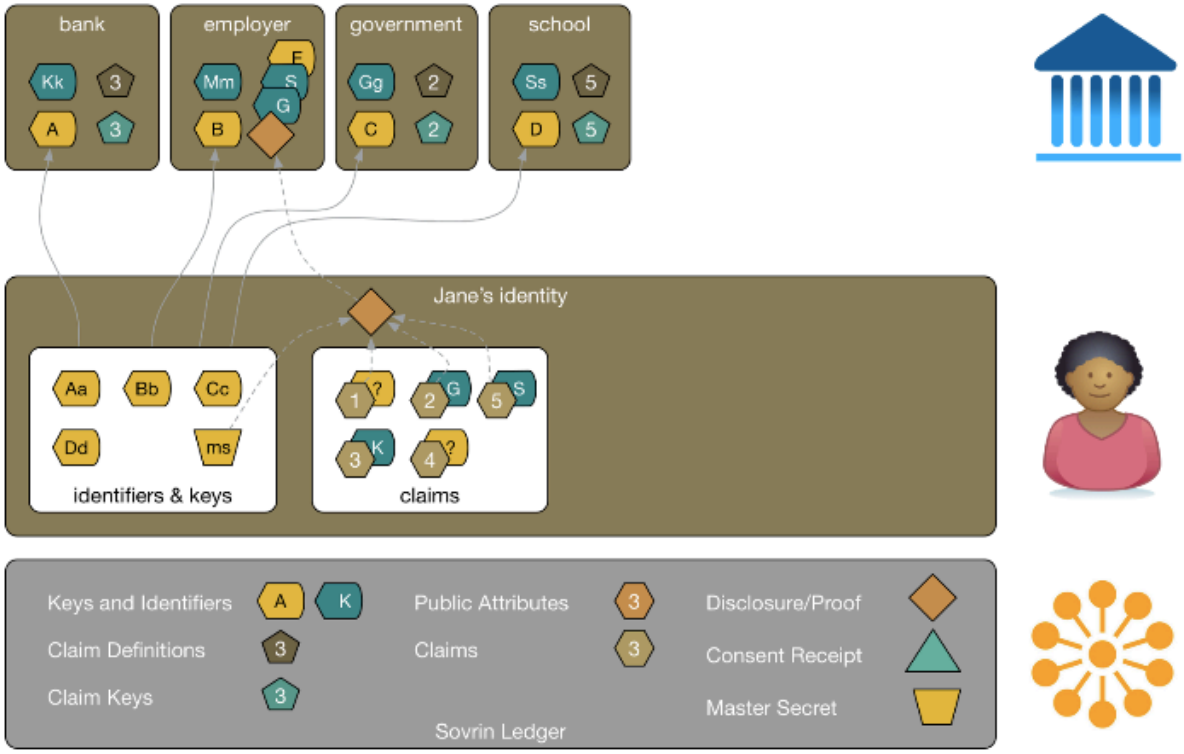
tiny fraction of the token to certify low value credentials. The higher the risk mitigated for a verifier (verifying a credit score needed for a loan), the higher the price paid.

The Sovrin token also introduces the idea of insurance on the claims made. Sovrin takes the example of a university that goes through an extensive accreditation process, yet fake diploma producers make $300M annually.[72] Instead of having employers need to verify authenticity of each educational institution, they can just trust the insurers that universities pay for in Sovrin tokens.

Another advantage of the Sovrin token over a project like the CVC token stems from the permissioned nature of the blockchain. In the case of changing addresses for 40 million Americans that move every year, each change costs approximately $6. These changes cost businesses billions of dollars a year in attempting to secure and verify the changes.[73][74] Since Sovrin is a permissioned blockchain, the Post Office could directly verify the address change and businesses can pay them and reward the identity owner in the form of tokens.[75]

[72] Sovrin Identity for All.
[73] "How Much Did Your Address Change Cost You?," accessed April 9, 2019, https://www.cbsnews.com/news/how-much-did-your-address-change-cost-you/.
[74] Sovrin Identity for All, "Sovrin™: A Protocol and Token for SelfSovereign Identity and Decentralized Trust."
[75] Koda Vista, "Trying to Understand the Sovrin Token Utility," *Koda Vista* (blog), July 11, 2018, https://medium.com/@kodavista/trying-to-understand-the-sovrin-token-utility-4727d0e987f1.

This ecosystem is depicted by the Sovrin network in the image below.[76]



Jane discloses attributes about her claims

In this scenario, Jane applies for a job and needs to verify the information from her school, government, and bank. Her box of claims contains claims she has self-asserted, perhaps her name and gender, and then claims from each of the other entities (address, age, degree). For her application, Jane can pick which claims she would like to disclose and form the proof needed to share with the employer. Each claim is paired with a verification key, that way when the entire proof is shared with the employer, the employer can validate that the claims were verified by the school, government, and bank. The added security feature lies in the fact that the employer and the

[76] Sovrin Foundation, "How Sovrin Works," Sovrin Foundation, October 3, 2016, https://blog.sovrin.org/how-sovrin-works-a1dff156c68e.

government cannot collude to reveal new information about Jane as the identifier she has with government does not correlate at all to the identifier she has with the employer. This would prevent someone working at the government to use information in the proof to try and get their friend at the employer to search up more information on Jane as her identifier would not correlate to anything on the other system.[77]

Drawbacks

One of the major drawbacks unique to Sovrin's platform remains the absence of a working application. The user experience determines the rate of adoption and viability of the product. The cryptographic nature of the technology allows for immense security advantages, but if no one knows how to use the app then none of the benefits including the credentials marketplace or insurance sales can ever take place. uPort and Civic both have launched applications that show promise in simplicity for users. Without this level of simplicity or understanding many users might find it hard to trust such a system with their credentials. Research suggests that "approaches to digital identity that remove central authorities depend on effective key management strategies from its users create the risk that non-technical users will be alienated by the technology; and when things go wrong those users will be unable to recover resources or reputation attached to lost keys."[78]

Review

All together Sovrin addresses many of the key privacy and trust issues in identity management. The public nature of the network allows for universalized usage. Since the network remains permissioned, Sovrin's governance and rules for the network can hold stewards and

[77] Foundation.
[78] Rachna Dhamija and Lisa Dusseault, "The Seven Flaws of Identity Management: Usability and Security Challenges," *IEEE Security & Privacy* 6 (2008), https://doi.org/10.1109/MSP.2008.49.

agencies legally accountable, differentiating Sovrin from other identity projects. The usages of new digital identifiers for each relationship enhances privacy as it mitigates risk of correlation when reusing identities.

Applications of Technology and Analysis

(Proof of Identity use cases infographic by the Boston Consulting Group and Australia Post)[79]

Building Blocks, World Food Programme and the United Nations

In 2016 the United Nations (UN) and World Food Programme (WFP) began developing a private, permissioned blockchain to deploy for use in refugee camps as a means of distributing cash for food aid.[80] The proof of concept was launched in 2017 in the Sindh province of Pakistan

[79] Boston Consulting Group Australia Post, "A Frictionless Future for Identity Management - A Practical Solution for Australia's Digital Identity Challenge," December 2016, https://auspostenterprise.com.au/content/dam/corp/ent-gov/documents/digital-identity-white-paper.pdf.
[80] "Blockchain for Zero Hunger | WFP Innovation," accessed April 11, 2019, /project/building-blocks.

and then later deployed to Azrkak refugee camp for Syrian refugees in Jordan. The WFP transferred a record high of $1.74 billion in cash transfers in 2018 to help refugees in across 62 different countries; this large volume of transfers results in extremely high financial costs that the program attempted to solve by using blockchain.[81]

Problem

In the past the WFP directly distributed food to beneficiaries but suffered from many setbacks including mistiming of delivery resulting in beneficiaries going without food at times.[82] The program switched to cash-based intervention where beneficiaries felt more dignified with their ability to purchase food and cater to their specific needs for consumption. This allowed for local economies to benefit as well as businesses and communities to benefit from the multiplier effect. Sustaining cash based intervention remained challenging however as the process involved lots of friction since beneficiaries and the WFP had to create bank accounts and go through the KYC process. The WFP would then work with banks to verify accounts and then maintain and crosscheck spending claims with shops, a cumbersome process to avoid losing funds to corruption. This process resulted in funds lost to transaction fees, lag time in transaction verification, and administrator delays. The impact remains large as upwards of 30% of UN assistance is lost to corruption.[83]

Technology

The private, permissioned blockchain runs on a fork of the Ethereum blockchain. The blockchain end of the platform links the WFP funding for beneficiaries directly to their cash

[81] "Cash Transfers | World Food Programme," accessed April 12, 2019, https://www1.wfp.org/cash-transfers.
[82] Ethereum Foundation, *Blockchain for Humanitarian Assistance*, accessed April 11, 2019, https://www.youtube.com/watch?time_continue=5&v=y50C2JEZMrQ.
[83] "Inside the Jordan Refugee Camp That Runs on Blockchain - MIT Technology Review."

provisions. The authorization of payment occurs when beneficiaries scan their iris' at the register, "once a shopper has their iris scanned, the system automatically communicates with UNHCR's registration database to confirm the identity of the refugee, checks the account balance with Jordan Ahli Bank and Middle East Payment Services and then confirms the purchase and prints out a receipt – all within seconds."[84] Now the WFP does not need to set up individual bank accounts for each beneficiary, rather they take their ledger of all transactions and through one bank transaction can pay the store all at once, a much cheaper process than before.[85]

[84] "WFP Introduces Iris Scan Technology To Provide Food Assistance To Syrian Refugees In Zaatari | World Food Programme," accessed April 13, 2019, https://www1.wfp.org/news/wfp-introduces-innovative-iris-scan-technology-provide-food-assistance-syrian-refu.
[85] Ethereum Foundation, *Blockchain for Humanitarian Assistance*.

(Customers pay for groceries at supermarkets in the Zaatari and Azrak refugee camps)[86][87]

The nature of having the WFP as a validator allows to speed up and scale more transactions at a much cheaper rate than if the WFP utilized a public blockchain. A public blockchain allows for a more democratic process of a truly decentralized network, thousands of nodes operating as validators cannot rewrite the transactions and no one party directly governs the process. Although these benefits primarily constitute the arguments for why agencies employ blockchain, the deployment of Building Blocks would cost too much if run on the public Ethereum main net. The gas and associated fees needed to process millions and billions of transactions would undermine

[86] "Inside the Jordan Refugee Camp That Runs on Blockchain - MIT Technology Review."
[87] "Blockchain for Zero Hunger | WFP Innovation."

the cost savings that prompted the WFP to use blockchain in the first place. The transaction throughput would be too much for the public chain. Branching off from the main Ethereum blockchain and creating a Proof of Authority Consensus algorithm for the private blockchain is how the WFP keeps costs low.

Proof of Authority is a modified version of the Proof of Stake model, it replaces tokens with identity as the form of stake in the network. This way a select few validators (WFP) can approve blocks in the network. The majority of the validators must sign off on the blocks. This system works well for a consortium network since a hacker cannot overwhelm the network and the process is less computationally intensive than traditional stake or work consensus algorithms.[88] In the case for the WFP, the blockchain currently only has one validator, the WFP. This begs the question, should the WFP use a proprietary database instead, why utilize blockchain technology? Houman Haddad, the main developer of the Building Blocks program argues that the fragmentation and duplication in the current UN humanitarian systems. He provides the example of a beneficiary, Bob, who receives aid from four different UN agencies. Each UN Agency operates with a different system and a different bank that do not connect or communicate with each other, meaning that Bob and the agencies maintain four different identities and account chains for the same person. This process remains a financial and time burden.[89] The advantages of blockchain technology come from the open source and flexible nature of the system, lessening ownership disputes since no one agency owns it. The system also allows for interoperability amongst systems as all the agencies can link to the same blockchain. A system on blockchain can scale to combine loans, remittances, food aid and investments all on the same network. This in

[88] "Parity Documentation - Proof-of-Authority Chains," accessed April 13, 2019, http://wiki.parity.io/Proof-of-Authority-Chains.html.
[89] Ethereum Foundation, *Blockchain for Humanitarian Assistance*.

turn increases the portability of the beneficiaries' identity as picking up and moving becomes remarkably easier with an integrated system.

Impacts

In the first five months of the program's deployment in the Azrak Refugee camp in Jordan, Building Blocks integrated over 10,500 beneficiaries into their system, recording over 200,000 transactions and $1.6 million in distributions.[90] The use of blockchain technology reduced the times and costs associated with banks, dropping the programs fees by 98% and saving the agency $150,000 a month.[9192] Over 500,00 refugees now utilize the program.

Economically speaking the project still faces some adoption challenges. The WFP claims that the 80 million people they serve can all be transitioned to a platform like Building Blocks.[93] One of the challenges for Building Block's widespread implantation lies in the fact that currently only two officially sanctioned grocery stores that accept payments using Building Blocks. The MIT Technology review finds that plenty of mom and pop vendors still operate as black market shops and Building Blocks has no infrastructure there.[94] If the operations remain centralized to only a few stores than the system gains no traction overall and stays a controlled database for a few shops than an actual decentralized platform.

Critics including Zara Rahman of the Berlin based organization, The Engine Room, warn "it is essential for human rights workers to stay critical and see past the hype. Though a certain tool might seem like the easiest option now, what about in two years or five years time? What will

---

[90] Ethereum Foundation.
[91] "Inside the Jordan Refugee Camp That Runs on Blockchain - MIT Technology Review."
[92] Stephen O'Neal, "DLT in Migration Policy: How Blockchain Can Help Both Refugees and Host Nations," Cointelegraph, September 19, 2018, https://cointelegraph.com/news/dlt-in-migration-policy-how-blockchain-can-help-both-refugees-and-host-nations.
[93] Ethereum Foundation, *Blockchain for Humanitarian Assistance*.
[94] "Inside the Jordan Refugee Camp That Runs on Blockchain - MIT Technology Review."

you want to do with the data, and who owns it?"[95] Houman Haddad claims that the project aims to expand to encompass a complete ID system where users can have a public-private key pair to sign off an authorize transactions as well as fully control data rights. The issue as of now centers around the lack of hardware and stable internet access in this region. In the future, with cheaper and more ubiquitous smartphones, along with potential free worldwide internet access, blockchain can onboard many refugees on a Civic/uPort or Sovrin like platform. The project hopes to serve as a proof of concept for other UN organizations to demonstrate the potential of blockchain technology and hopes to eventually incorporate work permits, visas, education history and other important credentials to ensure the safety and mobility of distressed populations.[96]

As witnessed with the Building Blocks pilot program, blockchain technology has the power to restore identity and dignity to refugees and many of the world's distressed populations. A secure identity platform or even a payments distribution network grants higher security, transparency and trust in humanitarian systems. The Syrian Refugee crisis is one of many instances where aid serves as a key stabilizer for millions on the run.[97] In the United States, fear that corruption and interception of funds by banks and unfriendly regimes will end up sponsoring terrorism or simply going to waste has undermined support for foreign aid projects. Studies have shown "that in personalist regimes US aid significantly increases levels of terrorist activity."[98] Many regimes further instability to continue receiving foreign aid as it is easily exploitable. In 2019 the proposed

[95] "Blockchain Could Change the Future of Humanitarian Aid," *Food Tank* (blog), January 3, 2019, https://foodtank.com/news/2019/01/the-world-food-program-fighting-hunger-with-blockchain/.
[96] Ethereum Foundation, *Blockchain for Humanitarian Assistance*.
[97] "Why Cutting Foreign Aid Benefits Terrorists," Council on Foreign Relations, accessed April 17, 2019, https://www.cfr.org/blog/why-cutting-foreign-aid-benefits-terrorists.
[98] Andrew Boutton, "Of Terrorism and Revenue: Why Foreign Aid Exacerbates Terrorism in Personalist Regimes," *Conflict Management and Peace Science*, December 21, 2016, 0738894216674970, https://doi.org/10.1177/0738894216674970.

budget for 2020 called for cuts to USAID and international developmental assistance programs funding by 24%, around $9 billion.[99]

A system such as Building Blocks exemplifies how aid can securely be distributed directly to individuals for food purchases. Replacing cash distribution with blockchain-based food purchases do not allow for funds to flow to illicit organizations. Administering aid through these measures can even prevent instability from breaking out in the first place as the economic empowerment of disenfranchised individuals can reduce how terrorist groups capitalize on the promises to empower marginalized groups against elites or foreigners.[100]

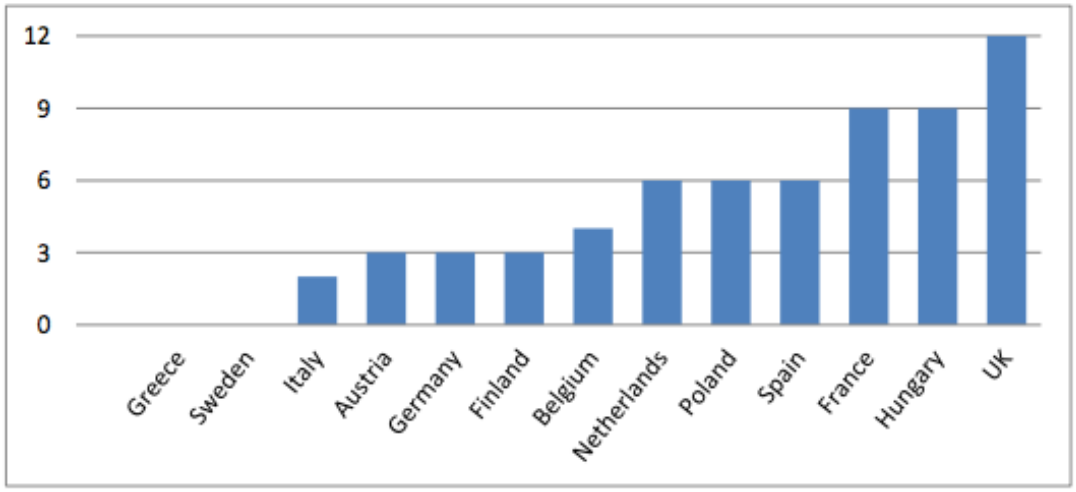
Self-Sovereign Identity for Migrant Refugees

The UNHCR High Commissioner states that "Syria is the biggest humanitarian and refugee crisis of our time" with over 5.6 million registered refugees outside of Syria. [101][102] The Norwegian Refugee Council found that 70% of Syrian refugees lacked basic identity documents, such as their national ID card, with 50% of married refugees lacking marriage documentation.[103] The study claims that the crisis is "threatening to leave hundreds of thousands in legal limbo, with dire consequences for their ability to access services and have a durable return to Syria." [104] The lack of any form of identification makes resettling in a new nation difficult. During the peak of the migration crisis (2015-16) about 1.2 million asylum seekers registered in Germany, with 23% of

[99] "Budget Calls for Deep Cuts to Foreign Aid, Especially for Refugees and in Humanitarian Crises - The Washington Post," accessed April 17, 2019, https://www.washingtonpost.com/.
[100] "Why Cutting Foreign Aid Benefits Terrorists."
[101] United Nations High Commissioner for Refugees, "Syria Emergency," UNHCR, accessed April 17, 2019, https://www.unhcr.org/syria-emergency.html.
[102] "Situation Syria Regional Refugee Response," accessed April 17, 2019, https://data2.unhcr.org/en/situations/syria#_ga=2.218694105.15037741.1555545225-2090702104.1553611614.
[103] "Syrian Refugees' Documentation Crisis," NRC, accessed April 17, 2019, https://www.nrc.no/news/2017/january/syrian-refugees-documentation-crisis/.
[104] "Syrian Refugees' Documentation Crisis."

applicants originating from Syria.[105] In this same timeframe of around one year, only 13% of refugees had found work.[106] Studies find that asylum seekers require documentation processing and they must obtain work permits, generating "administrative burden" on the host country, which deters employers from hiring them.[107] Per EU Directive 2013/33 Member states must ensure that asylum seekers access the labor market no later than 9 months after they apply for protection. This timeframe also allows for states to decide minimum waiting periods from when asylum seekers apply to when they can access the labor market for the states to handle the administrative work.

Figure 6: Minimum waiting periods for accessing the labour market for asylum seekers*, in months, 2017



(Taken from European Union Parliament Directorate General for Internal Policies)[108]

Asylum seekers have a harder time entering the labor market and settling due to the difficulty in processing requests and authorizing permits for a population without any form of identity. Foreign credentials can significantly reduce latency in application processing and also

[105] Regina Konle-Seidl, "Integration of Refugees in Austria, Germany and Sweden: Comparative Analysis," n.d., 63.
[106] "Only 13 Percent of Recent Refugees in Germany Have Found Work: Survey," *Reuters*, November 15, 2016, 14, https://www.reuters.com/article/us-europe-migrants-germany-survey-idUSKBN13A22F.
[107] Konle-Seidl, "Integration of Refugees in Austria, Germany and Sweden: Comparative Analysis."
[108] Konle-Seidl.

directly improve employment prospects. The German Institute for Economic Research found that "immigrants (including refugees) with foreign degrees being recognised as equivalent to home country degrees improve their employment rate by 23 percentage points, reduce job-skills mismatch by 32 percentage points and increase their wages by 28 % compared to those immigrants who did not ask for recognition."[109] In Germany, nine out of ten migrants with a foreign professional qualification are employed after the successful recognition of their qualifications, which means that the employment rate rises sharply by over 50% and the gross income increases by an average of €1,000 a month.[110] The German Federal Office for Migration and Refugees also grants an extended residence permit for six months for individuals with a foreign higher education qualification or German higher education.[111]

A blockchain-based digital identity system can serve as the solution for asylum seekers and governments alike. The administrative burden placed on governments trying to verify asylum claims and also identity documentation places high costs on societies. The lack of documentation for Syrian refugees while traveling makes applications even more difficult and further makes returning post crisis logistically challenging.

One possible solution utilizes the Sovrin Network, where specific stewards, such as the UNHCR, European governments and other authorities can serve as validators for identification. Another system could utilize the ID scanning verification that Civic utilizes to scan existing national identity documentation, degrees, and permits that individuals already have.

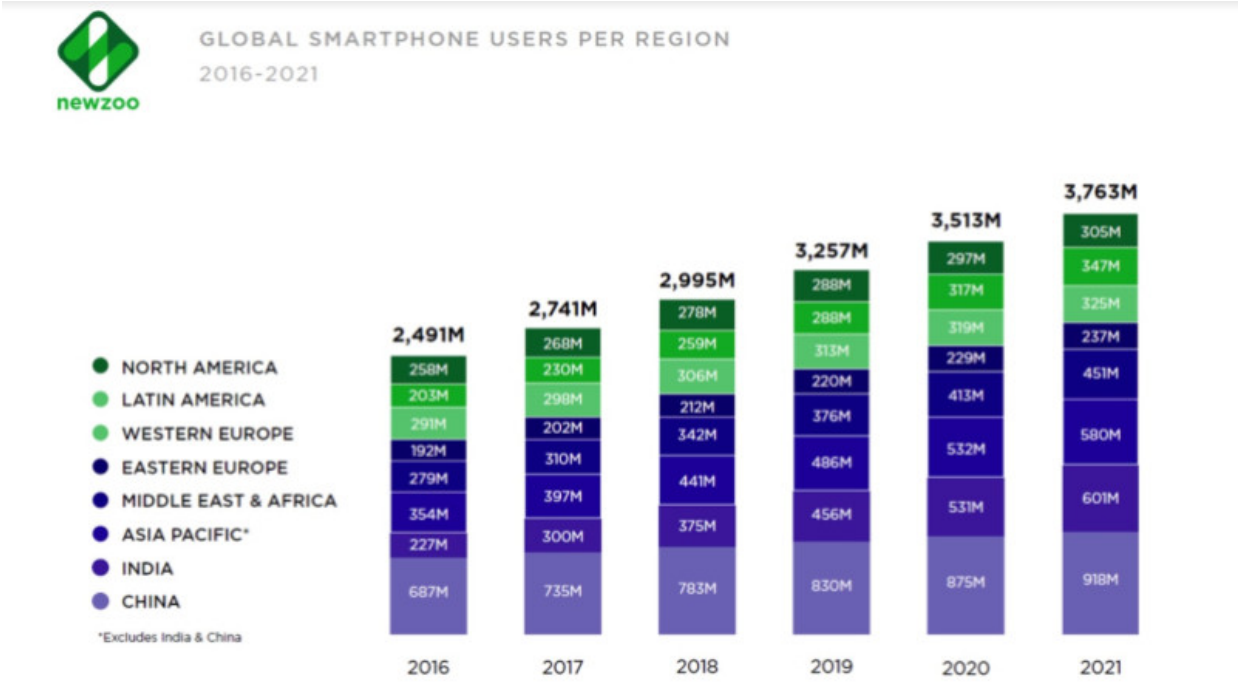
---

[109] Herbert Brücker et al., "The New IAB-SOEP Migration Sample: An Introduction into the Methodology and the Contents," n.d., 23.
[110] "Bericht zum Anerkennungsgesetz 2017," n.d., 78.
[111] "Job-Seekers," Bundesamt für Migration und Flüchtlinge, accessed April 17, 2019, http://www.bamf.de/EN/Migration/Arbeiten/BuergerDrittstaat/Arbeitsplatzsuche/arbeitsplatzsuche-node.html.

The blockchain storage of these attestations can speed up the process of refugee resettlement in the host countries. In the case of Germany, the economic impacts quantify in the form of 28% higher wages for verified degree holders and faster permit processing times as the government has biometric and blockchain backed verification of identity. Ethereum smart contracts can facilitate secure and recorded spending of entitlement benefits where the issuing government authority can allocate funds to a wallet and purchases of specific goods such as medical supplies or groceries trigger the release of those funds. Smart contracts can automatically pay taxes upon administered wages, authorize school lunch payments after a school logs attendance for a student and so on.

One of the biggest setbacks to full scale adoption of such a system remains smartphone access and connectivity. As of 2018, worldwide smartphone penetration was estimated at 3 billion users, predicted to increase to 3.8 billion by 2021 with the largest share of growth coming from the developing world. Penetration in the United States is 77% and is highest in the United Kingdom at 82.2%.[112] Smartphone penetration in conflict torn countries, arguably where self-sovereign identity can have the greatest impact on lives, remains rather low. Pakistan stands at 13.8%, Sudan at 19.7%, and Ethiopia at 11.2%, and all three of these countries still rank in the top 50 countries worldwide for smartphone penetration.[113] Smartphones serve as one of the easiest methods for users to interact with and manage their identity. Methods like iris scanning can still benefit individuals, but mass engagement of self-sovereign identity seems difficult without a smartphone.

[112] "Newzoo: Smartphone Users Will Top 3 Billion in 2018, Hit 3.8 Billion by 2021," *VentureBeat* (blog), September 11, 2018, https://venturebeat.com/2018/09/11/newzoo-smartphone-users-will-top-3-billion-in-2018-hit-3-8-billion-by-2021/.
[113] "Newzoo."



(Taken from Newzoo study)[114]

Universal adoption of a blockchain-based identity solution such as Sovrin prior to the breakout of an international migration crisis could mitigate many of the current issues faced by refugees. Having titles, records and identity tracked on a verified and immutable ledger can help ease immigration but also ease the return of refugees home. Following the settlement of a war or crisis, those who chose to return home have no way of verifying elements of their past lives. A new post-war government might not have the infrastructure or log of records to verify claims to land and licenses prior to conflict. Having these claims verified and stored on the blockchain ensures credibility and longevity of such claims, making resettlement much easier. Blockchain technology allows for a more humane immigration process by increasing transparency, individual agency, and efficiency.

[114] "Newzoo."

Human Trafficking

The 1.1 billion people today that lack a form of identity become legally invisible where the likelihood that their disappearance and exploitation will go unnoticed by authorities becomes much greater.[115][116] Without any form of documentation or registration of existence disadvantaged individuals including children, economic migrants, individuals fleeing abuse, become vulnerable to human traffickers that can use fake ID documents to transfer them internationally and exploit them for sex, labor and organs. This portion of the paper will detail the scope of modern-day slavery and then offer blockchain based identity solutions.

The International Labor Organization estimates that 24.9 million victims are trapped in modern-day slavery, earning profits of nearly $150 billion.[117] Of these profits, $99 billion come from sexual exploitation, and 71% of all victims are women and girls; 25% of the victims are children under the age of 18.[118] In the majority of trafficking cases victims are moved across international borders, mostly within the same region of the world. Traffickers rely on faulty border security and poor identification systems to forge documentation to cross international borders. In systems where trust in physical documents cannot be established, blockchain presents an opportunity for digital identity that is nearly impossible to forge. One possibility includes combining biometrics, such as a fingerprint or iris scan with a blockchain identity instead of a paper document to verify individual identities.

---

[115] "1.1 Billion 'Invisible' People without ID Are Priority for New High Level Advisory Council on Identification for Development."
[116] World Identity Network, London School of Economics, and UNOPS, "TURNING INVISIBLE CHILDREN INTO INVINCIBLE ONES," accessed April 23, 2019, https://win.systems/wp-content/uploads/2018/09/blockchain-for-humanity-1.pdf.
[117] International Labour Office and Special Action Programme to Combat Forced Labour, *Profits and Poverty: The Economics of Forced Labour.*, 2014.
[118] International Labour Office and Special Action Programme to Combat Forced Labour.

Forced labor usually begins through direct force or through deceit/coercion; deceit typically occurs when desperate workers in poorer regions get lured in by traffickers presenting job opportunities with the promises of higher wages and success in a foreign country.[119] Since a large portion of these victims do not have any form of identification, traffickers use forged identities to transport victims. These victims end up in a foreign country with no paperwork and means of getting back and can be kept in slavery indefinitely by the threat of violence or coercion.[120] The following will analyze a possible use case of blockchain technology to combat trafficking in the Thai fishing industry.

Thai Fishing Industry

In Thailand's fishing industry 76% of migrant workers had been held in debt bondage and 38% of them had been trafficked into the industry.[121] The exploitation of workers thrives off the lack of documented identity. Traffickers confiscate passports, identity cards and other documents, making the workers effectively virtual prisoners.[122] The distant water fishing requires the crew to travel to remote locations for extended periods of time.[123] Without any verified record of which workers are on the boat and for how long there is little oversight by any regulatory authorities. Regulatory authorities in lower GDP countries, even Thailand in this case, may have limited monitoring ability and corruption can even lead to forging of records of fish

---

[119] Siân Oram et al., "Prevalence and Risk of Violence and the Physical, Mental, and Sexual Health Problems Associated with Human Trafficking: Systematic Review," *PLoS Medicine* 9, no. 5 (May 2012): 1–13, https://doi.org/10.1371/journal.pmed.1001224.
[120] Sarah R. Meyer et al., "Trafficking, Exploitation and Migration on the Thailand-Burma Border: A Qualitative Study," *International Migration* 53, no. 4 (August 2015): 37–50, https://doi.org/10.1111/imig.12177.
[121] "Fishing," Global Slavery Index, accessed April 24, 2019, https://www.globalslaveryindex.org/2018/findings/importing-risk/fishing/.
[122] Alex Capri, "How Blockchain Could Help End Modern Day Slavery In Asia's Exploitative Seafood Industry," Forbes, accessed April 24, 2019, https://www.forbes.com/sites/alexcapri/2018/02/14/how-blockchain-could-help-end-modern-day-slavery-in-asias-exploitative-seafood-industry/.
[123] "Fishing."

caught or workers contracted to avoid penalties. The workers can be forced to work at length, often with little pay, since there is no way for them to leave. Debt bondage also occurs where workers are told they owe money to the employer for processing their employment and they cannot leave or have their documents back until they pay off the debt through labor. Thet Phyo Lin, a Burmese fisher recounts his experience: "If I want to quit working here I need to request permission from the employer. Some employers allow us to leave, but some will claim we must pay off debts first. For example, if I can pay 25,000 baht [US$762] to an employer … he may allow me to leave, but if he isn't satisfied … I would have to pay whatever he demanded."[124]

In situations of forced labor like above where the governing body has taken few steps for oversight and the validity of their claims cannot hold up due to prevalence of corruption, blockchain technology offers a solution to ensure permanent and uncompromised records to preserve human rights. Utilizing a program such as iRespond, that has already been used in Syria and Thailand, to scan irises and link them to a unique blockchain identity can prevent forged documents from working. Individuals then become traceable and verification can occur at ports or border to record workers time at sea.

In order to actually create this system, the governing bodies or companies must face pressure and requirements to comply with humane standards. This can occur if consumers or importers of the product demand transparency and fair practices. In 2015 the European Union threatened Thailand with a trade ban over its illegal fishing activity.[125] This prompted the Thai government to impose laws that required migrant fishers "to have legal documents and be

[124] Human Rights Watch, "Thailand: Forced Labor, Trafficking Persist in Fishing Fleets | Human Rights Watch," January 23, 2018, https://www.hrw.org/news/2018/01/23/thailand-forced-labor-trafficking-persist-fishing-fleets.
[125] Arthur Neslen, "EU Threatens Thailand with Trade Ban over Illegal Fishing," *The Guardian*, April 21, 2015, sec. Environment, https://www.theguardian.com/environment/2015/apr/21/eu-threatens-thailand-with-trade-ban-over-illegal-fishing.

accounted for on crew lists as boats departed and returned to port, helping to end some of the worst abuses, such as captains killing crew members. Thailand also created the Port-in, Port-out (PIPO) system to require boats to report for inspections as they departed and returned to port, and established procedures for inspection of fishing vessels at sea."[126] (these measures, however, have not created an effective inspection system for fishers working on the vessels). Thailand's 2015 report on human trafficking "inspections of 474,334 fishery workers failed to identify a single case of forced labor", and more recently in 2018 found no violations in 50,000 implausible inspections.[127][128] The laws might sound robust but the enforcement lacks.

Blockchain allows for trust to be stored in the network of validators and not the records of the government. The US and the EU have put pressure on these practices in the past, and the government responded with some improvements but trafficking still runs rampant. Regulations imposed on the end of the importers can prompt businesses to force their suppliers to comply with fair standards. The iris scanning system can work as one example where suppliers either pressure the Thai government to verify crews entering or exiting ports or simply institute the policy themselves. In 2015 Nestle audited its Thai seafood supply chains, uncovering labor abuses in the industry.[129] Corporations like Nestle can improve transparency and reduce costs in their supply chain by administering payments through blockchain, which would transition the middlemen and suppliers to integrate onto the platform. Transitioning the supply chain enterprise resource planning might not be an easy task but can save an enormous amount as seen with the

[126] Human Rights Watch, "Thailand: Forced Labor, Trafficking Persist in Fishing Fleets | Human Rights Watch."
[127] The Royal Thai Government, "TRAFFICKING IN PERSONS REPORT 2015|The Royal Thai Government's Response," 2015, http://ccpl.mol.go.th/ewt_dl_link.php?nid=86&.
[128] Human Rights Watch, "Thailand: Forced Labor, Trafficking Persist in Fishing Fleets | Human Rights Watch."
[129] Capri, "How Blockchain Could Help End Modern Day Slavery In Asia's Exploitative Seafood Industry."

World Food Programme. For those committed to fighting human trafficking, especially in labor practices, empowering workers with a self-sovereign identity can allow for workers to get automatically paid per their actual contract and have the freedom to leave without fear of their identity being confiscated. Most importantly, blockchain identity can assist officials in stopping traffickers from utilizing illegal documentation to pass checkpoints. Ultimately, the success of these technologies can be undermined by corruption and simply bribing authorities. For those committed to security, the technology holds significant potential.

Conclusion

There is no doubt that blockchain technology has the potential to disrupt many industries. This paper focuses on the application for blockchain in digital identity. Current forms of identity have many drawbacks; physical identity can be forged, destroyed and misplaced. Digital identity through the forms of centralized authorities, such as E-mail or social media accounts, offer a persistent experience with easy logging in with the tradeoff of little credibility and data privacy issues. Blockchain identity through the likes of uPort, Civic, and Sovrin each offer a digital identity solution that can create an entire ecosystem where verified claims to identity can be managed and transacted upon. For individuals, this means control over data usage and heightened security as decentralization makes attacks much more difficult. For enterprises and governments, self-sovereign identity could reduce risk of transacting with fraudulent and malicious actors for both high and low level credentials.

Blockchain-based digital identity has shown some promise through the World Food Programme's Building Blocks project where administrative costs fell 98% and biometric-linked identity integrated over 500,000 refugees. Unfortunately, without an entire ecosystem with hundreds of thousands of validators on a blockchain network, public or permissioned, the

Building Blocks system functions like a database. Self-sovereign identity deployment in the forms presented by uPort, Civic, and Sovrin is limited by internet connectivity, smartphone penetration and users on the network. Human governance is still necessary to ensure legal liability for fraudulent validators on a network – Sovrin provides a framework for this. The Estonian government pioneers a larger onboarding of millions of users but still lacks credibility and international recognition.

The advantages of blockchain digital identity provide incredible benefits to migrant refugees and victims of trafficking. The ability to store certified claims such as degrees, licenses or any identity claims could drastically cut down administrative strain for governments processing asylum requests. Digital identity can prevent fraud in immigration and can assist returning refugees validate their records upon returning home. For trafficking victims, biometrics linked to blockchain identity can reduce the likelihood of forged documentation assisting in border crossings and can prevent employers from holding humans captive by stealing passports or other forms of identity.

Blockchain can serve as a viable solution for the global identity crisis. Its adoption depends heavily on the quantity of users joining and the network effects linked to that. This process relies on an easy to use interface and support from credible authorities such as governments, multinational NGO's, and accredited institutions. The technology has the potential to empower individuals to take back control of their identity.

Bibliography

"1.1 Billion 'Invisible' People without ID Are Priority for New High Level Advisory Council on Identification for Development." Text/HTML. World Bank. Accessed March 26, 2019. http://www.worldbank.org/en/news/press-release/2017/10/12/11-billion-invisible-people-without-id-are-priority-for-new-high-level-advisory-council-on-identification-for-development.

Anapol, Avery. "Obama on His Criticism of Israeli Settlements: 'I'm Basically a Liberal Jew.'" Text. TheHill, January 26, 2018. https://thehill.com/blogs/blog-briefing-room/370947-obama-on-his-criticism-of-israeli-settlements-im-basically-a-liberal-jew.

"Anonymous Age Checks." Civic Technologies, Inc. Accessed March 26, 2019. https://www.civic.com/solutions/vending-machines/.

Aublin, Pierre-Louis, Sonia Ben Mokhtar, and Vivien Quema. "RBFT: Redundant Byzantine Fault Tolerance." In *2013 IEEE 33rd International Conference on Distributed Computing Systems*, 297–306. Philadelphia, PA, USA: IEEE, 2013. https://doi.org/10.1109/ICDCS.2013.53.

"Austin Is Piloting Blockchain to Improve Homeless Services." *TechCrunch* (blog). Accessed March 26, 2019. http://social.techcrunch.com/2018/04/14/austin-is-piloting-blockchain-to-improve-homeless-services/.

Australia Post, Boston Consulting Group. "A Frictionless Future for Identity Management - A Practical Solution for Australia's Digital Identity Challenge," December 2016. https://auspostenterprise.com.au/content/dam/corp/ent-gov/documents/digital-identity-white-paper.pdf.

"Bericht zum Anerkennungsgesetz 2017," n.d., 78.

"Bitnation and Estonian Government Start Spreading Sovereign Jurisdiction on the Blockchain." International Business Times UK, November 28, 2015. https://www.ibtimes.co.uk/bitnation-estonian-government-start-spreading-sovereign-jurisdiction-blockchain-1530923.

"Blockchain Could Change the Future of Humanitarian Aid." *Food Tank* (blog), January 3, 2019. https://foodtank.com/news/2019/01/the-world-food-program-fighting-hunger-with-blockchain/.

"Blockchain for Zero Hunger | WFP Innovation." Accessed April 11, 2019. /project/building-blocks.

"Blockchains (Continued) | Distributed Ledger Technology (DLT) | LFS171x Courseware | EdX." Accessed March 26, 2019. https://courses.edx.org/courses/course-v1:LinuxFoundationX+LFS171x+3T2017/courseware/4bdba535373943059204 3585c7fbf044/bf7a3e04813b46e79773b5b55f339861/6?activate_block_id=block-v1%3ALinuxFoundationX%2BLFS171x%2B3T2017%2Btype%40html%2Bblock%400957d77a70354ae5beed429603a4da4a.

Boutton, Andrew. "Of Terrorism and Revenue: Why Foreign Aid Exacerbates Terrorism in Personalist Regimes." *Conflict Management and Peace Science*, December 21, 2016, 0738894216674970. https://doi.org/10.1177/0738894216674970.

Braendgaard, Pelle. "What Is a UPort Identity?" *UPort* (blog), February 27, 2017. https://medium.com/uport/what-is-a-uport-identity-b790b065809c.

———. "What Is a UPort Identity?" *UPort* (blog), February 27, 2017. https://medium.com/uport/what-is-a-uport-identity-b790b065809c.

Brücker, Herbert, Andreas Hauptmann, Elke J. Jahn, and Richard Upward. "Migration and Imperfect Labor Markets: Theory and Cross-Country Evidence from Denmark, Germany and the UK." *European Economic Review* 66 (February 2014): 205–25. https://doi.org/10.1016/j.euroecorev.2013.11.007.

Brücker, Herbert, Martin Kroh, Simone Bartsch, Jan Goebel, Simon Kühne, Elisabeth Liebau, Parvati Trübswetter, Ingrid Tucci, and Jürgen Schupp. "The New IAB-SOEP Migration Sample: An Introduction into the Methodology and the Contents," n.d., 23.

"Budget Calls for Deep Cuts to Foreign Aid, Especially for Refugees and in Humanitarian Crises - The Washington Post." Accessed April 17, 2019. https://www.washingtonpost.com/.

Burke, Jamie. “WHY WE ARE BACKING EVERNYM & THE SOVRIN FOUNDATION.” *Outlier Ventures* (blog), October 22, 2017. https://medium.com/outlier-ventures-io/why-we-are-backing-evernym-the-sovrin-foundation-1822d2804991.

“Canada Tests Biometrics and Blockchain as Airports Worldwide Extend Biometric Use.” *Biometric Technology Today* 2018, no. 2 (February 1, 2018): 11–12. https://doi.org/10.1016/S0969-4765(18)30026-2.

Capri, Alex. “How Blockchain Could Help End Modern Day Slavery In Asia’s Exploitative Seafood Industry.” Forbes. Accessed April 24, 2019. https://www.forbes.com/sites/alexcapri/2018/02/14/how-blockchain-could-help-end-modern-day-slavery-in-asias-exploitative-seafood-industry/.

“Cash Transfers | World Food Programme.” Accessed April 12, 2019. https://www1.wfp.org/cash-transfers.

“Civic Decentralized Reusable KYC Services - Blockchain-Powered.” Civic Technologies, Inc. Accessed March 28, 2019. https://www.civic.com/solutions/kyc-services/.

“Civic Identity Verification Crowdsale.” Accessed March 28, 2019. https://tokensale.civic.com/.

“Civic Reusable Know Your Customer (KYC) - Decentralized via Blockchain.” Civic Technologies, Inc. Accessed March 28, 2019. https://www.civic.com/products/reusable-kyc/.

Civic Technologies. “Civic Token Sale WhitePaper.” Accessed March 26, 2019. https://tokensale.civic.com/CivicTokenSaleWhitePaper.pdf.

“Council Post: Know Your Customer (KYC) Will Be A Great Thing When It Works.” Accessed March 31, 2019. https://www.forbes.com/sites/forbestechcouncil/2018/07/10/know-your-customer-kyc-will-be-a-great-thing-when-it-works/#110a4ac78dbb.

Dhamija, Rachna, and Lisa Dusseault. “The Seven Flaws of Identity Management: Usability and Security Challenges.” *IEEE Security & Privacy* 6 (2008). https://doi.org/10.1109/MSP.2008.49.

Dunphy, Paul, and Fabien A. P. Petitcolas. “A First Look at Identity Management Schemes on the Blockchain.” *ArXiv:1801.03294 [Cs]*, January 10, 2018. http://arxiv.org/abs/1801.03294.

e-estonia. *Estonian E-Residency’s First Anniversary*. Accessed March 26, 2019. https://www.youtube.com/watch?v=exyg1Eybcjw.

“ERC: Lightweight Identity · Issue #1056 · Ethereum/EIPs.” GitHub. Accessed March 26, 2019. https://github.com/ethereum/EIPs/issues/1056.

Ethereum Foundation. *Blockchain for Humanitarian Assistance*. Accessed April 11, 2019. https://www.youtube.com/watch?time_continue=5&v=y50C2JEZMrQ.

“Ewt_dl_link.Pdf.” Accessed April 24, 2019. http://ccpl.mol.go.th/ewt_dl_link.php?nid=86&.

“Fishing.” Global Slavery Index. Accessed April 24, 2019. https://www.globalslaveryindex.org/2018/findings/importing-risk/fishing/.

Foundation, Sovrin. “How Sovrin Works.” Sovrin Foundation Blog, October 3, 2016. https://blog.sovrin.org/how-sovrin-works-a1dff156c68e.

Fracassi, Cesare. “Intro to Cryptography FIN 294.” The University of Texas at Austin, Spring 2019.

GELB, ALAN, and ANNA DIOFASI METZ. “Identification Systems:: Innovations in Technology and ID Provision.” In *Identification Revolution*, 91–124. Can Digital ID Be Harnessed for Development? Brookings Institution Press, 2018. https://www.jstor.org/stable/10.7864/j.ctt21c4t40.8.

"How Human Trafficking Works." HowStuffWorks, May 17, 2011. https://people.howstuffworks.com/human-trafficking.htm.

"How Much Did Your Address Change Cost You?" Accessed April 9, 2019. https://www.cbsnews.com/news/how-much-did-your-address-change-cost-you/.

"How to Start a Company in Estonia & EU." *E-Residency* (blog). Accessed May 10, 2019. https://e-resident.gov.ee/start-a-company/.

Human Rights Watch. "Thailand: Forced Labor, Trafficking Persist in Fishing Fleets | Human Rights Watch," January 23, 2018. https://www.hrw.org/news/2018/01/23/thailand-forced-labor-trafficking-persist-fishing-fleets.

"Hyperledger Indy | Hyperledger Frameworks | LFS171x Courseware | EdX." Accessed March 26, 2019. https://courses.edx.org/courses/course-v1:LinuxFoundationX+LFS171x+3T2017/courseware/fa54f0debd00468695b36d6ce87dc070/6a977492dec44c32a9e80c8a29372104/11?activate_block_id=block-v1%3ALinuxFoundationX%2BLFS171x%2B3T2017%2Btype%40vertical%2Bblock%40baad2d38202d4a9db52a26a9066af2a7.

Iansiti, Marco, and Karim R. Lakhani. "The Truth About Blockchain." *Harvard Business Review*, January 1, 2017. https://hbr.org/2017/01/the-truth-about-blockchain.

"Inside the Jordan Refugee Camp That Runs on Blockchain - MIT Technology Review." Accessed March 26, 2019. https://www.technologyreview.com/s/610806/inside-the-jordan-refugee-camp-that-runs-on-blockchain/.

International Labour Office, and Special Action Programme to Combat Forced Labour. *Profits and Poverty: The Economics of Forced Labour.*, 2014.

"Job-Seekers." Bundesamt für Migration und Flüchtlinge. Accessed April 17, 2019. http://www.bamf.de/EN/Migration/Arbeiten/BuergerDrittstaat/Arbeitsplatzsuche/arbeitsplatzsuche-node.html.

Konle-Seidl, Regina. "Integration of Refugees in Austria, Germany and Sweden: Comparative Analysis," n.d., 63.

Labott, Elise. "Why Trump's Israel Ambassador Could Upend Middle East Ties - CNNPolitics," December 17, 2016. https://www.cnn.com/2016/12/17/politics/david-friedman-ambassador-to-israel-nominee/index.html.

Linum Labs. *ConsenSys and UPort: Powering Decentralized Identity*. Accessed March 26, 2019. https://www.youtube.com/watch?v=VXAZdBtN3N0.

Lucerne University of Applied Sciences and Arts. "Evaluation of the Blockchain Vote in the City of Zug," November 30, 2018, 6.

Lundkvist, Dr Christian, Rouven Heck, Joel Torstensson, Zac Mitton, and Michael Sena. "UPORT: A PLATFORM FOR SELF-SOVEREIGN IDENTITY," n.d., 17.

Meyer, Sarah R., W. Courtland Robinson, Nada Abshir, Aye Aye Mar, and Michele R. Decker. "Trafficking, Exploitation and Migration on the Thailand-Burma Border: A Qualitative Study." *International Migration* 53, no. 4 (August 2015): 37–50. https://doi.org/10.1111/imig.12177.

Nawfal, Alice. "Zug Residents Can Now Ride E-Bikes Using Their UPort-Powered Zug Digital IDs." *Medium* (blog), November 14, 2018. https://medium.com/uport/zug-residents-can-now-ride-e-bikes-using-their-uport-powered-zug-digital-ids-7ed31ac9d621.

Neslen, Arthur. "EU Threatens Thailand with Trade Ban over Illegal Fishing." *The Guardian*, April 21, 2015, sec. Environment. https://www.theguardian.com/environment/2015/apr/21/eu-threatens-thailand-with-trade-ban-over-illegal-fishing.

"Newzoo: Smartphone Users Will Top 3 Billion in 2018, Hit 3.8 Billion by 2021." *VentureBeat* (blog), September 11, 2018. https://venturebeat.com/2018/09/11/newzoo-smartphone-users-will-top-3-billion-in-2018-hit-3-8-billion-by-2021/.

O'Neal, Stephen. "DLT in Migration Policy: How Blockchain Can Help Both Refugees and Host Nations." Cointelegraph, September 19, 2018. https://cointelegraph.com/news/dlt-in-migration-policy-how-blockchain-can-help-both-refugees-and-host-nations.

"Only 13 Percent of Recent Refugees in Germany Have Found Work: Survey." *Reuters*, November 15, 2016. https://www.reuters.com/article/us-europe-migrants-germany-survey-idUSKBN13A22F.

Oram, Siân, Heidi Stoöckl, Joanna Busza, Louise M. Howard, and Cathy Zimmerman. "Prevalence and Risk of Violence and the Physical, Mental, and Sexual Health Problems Associated with Human Trafficking: Systematic Review." *PLoS Medicine* 9, no. 5 (May 2012): 1–13. https://doi.org/10.1371/journal.pmed.1001224.

"Parity Documentation - Proof-of-Authority Chains." Accessed April 13, 2019. http://wiki.parity.io/Proof-of-Authority-Chains.html.

Ray, Shaan. "Merkle Trees." Hacker Noon, December 15, 2017. https://hackernoon.com/merkle-trees-181cb4bc30b4.

Refugees, United Nations High Commissioner for. "Identity Documents for Refugees." UNHCR. Accessed March 26, 2019. https://www.unhcr.org/excom/scip/3ae68cce4/identity-documents-refugees.html.

———. "Syria Emergency." UNHCR. Accessed April 17, 2019. https://www.unhcr.org/syria-emergency.html.

Rush, Nate. "Making the UPort Smart Contracts Smarter." *UPort* (blog), August 14, 2017. https://medium.com/uport/making-the-uport-smart-contracts-smarter-e1798d8c1cf9.

Sarrica, Fabrizio, Anja Korenblik, and Suzanne Kunnen. “Research Coordination and Report Preparation:,” n.d., 292.

———. “Research Coordination and Report Preparation:,” n.d., 292.

———. “Research Coordination and Report Preparation:,” n.d., 292.

“Self-Sovereign Identity: Why Blockchain? - Blockchain Pulse: IBM Blockchain Blog.” Accessed March 31, 2019. https://www.ibm.com/blogs/blockchain/2018/06/self-sovereign-identity-why-blockchain/.

“Simplified Byzantine Fault Tolerance (SBFT) | Consensus Algorithms | LFS171x Courseware | EdX.” Accessed March 26, 2019. https://courses.edx.org/courses/course-v1:LinuxFoundationX+LFS171x+3T2017/courseware/4bdba535373943059204 3585c7fbf044/42a0909f1f6f4930a6501be2d72a5905/5?activate_block_id=block-v1%3ALinuxFoundationX%2BLFS171x%2B3T2017%2Btype%40vertical%2Bblock%40a17f832561fa4511ae4b933777175e69.

“Situation Syria Regional Refugee Response.” Accessed April 17, 2019. https://data2.unhcr.org/en/situations/syria#_ga=2.218694105.15037741.1555545225-2090702104.1553611614.

“Sovrin Governance Framework.” *Sovrin* (blog). Accessed April 7, 2019. https://sovrin.org/library/sovrin-governance-framework/.

Sovrin Identity for All. “Sovrin-Governance-Framework-V2-Master-Document-V1.Pdf,” 2019. https://sovrin.org/wp-content/uploads/2019/03/Sovrin-Governance-Framework-V2-Master-Document-V1.pdf.

———. “Sovrin™: A Protocol and Token for SelfSovereign Identity and Decentralized Trust,” January 2018. https://sovrin.org/wp-content/uploads/2018/03/Sovrin-Protocol-and-Token-White-Paper.pdf.

Sullivan, Clare, and Eric Burger. “E-Residency and Blockchain.” *Computer Law & Security Review* 33, no. 4 (August 1, 2017): 470–81. https://doi.org/10.1016/j.clsr.2017.03.016.

“Syrian Refugees’ Documentation Crisis.” NRC. Accessed April 17, 2019. https://www.nrc.no/news/2017/january/syrian-refugees-documentation-crisis/.

The Royal Thai Government. “TRAFFICKING IN PERSONS REPORT 2015|The Royal Thai Government’s Response,” 2015. http://ccpl.mol.go.th/ewt_dl_link.php?nid=86&.

“Thomson Reuters 2016 Know Your Customer Surveys Reveal Escalating Costs and Complexity.” Accessed March 29, 2019. https://www.thomsonreuters.com/en/press-releases/2016/may/thomson-reuters-2016-know-your-customer-surveys.html.

“Top Countries/Markets by Smartphone Penetration & Users.” *Newzoo* (blog). Accessed April 22, 2019. https://newzoo.com/insights/rankings/top-50-countries-by-smartphone-penetration-and-users/.

UN General Assembly. “United Nations Official Document, Transforming Our World: The 2030 Agenda for Sustainable Development.” Accessed March 26, 2019. http://www.un.org/ga/search/view_doc.asp?symbol=A/70/L.1&Lang=E.

“UPort Announces Zug Digital Ethereum ID Pilot.” ETHNews.com. Accessed March 26, 2019. https://www.ethnews.com/uport-announces-zug-digital-ethereum-id-pilot.

“UPort Controller Contracts.” Accessed March 26, 2019. https://developer.uport.meundefined/overview/index.

Vista, Koda. “Trying to Understand the Sovrin Token Utility.” *Koda Vista* (blog), July 11, 2018. https://medium.com/@kodavista/trying-to-understand-the-sovrin-token-utility-4727d0e987f1.

Vryonis, Panayotis. “Explaining Public-Key Cryptography to Non-Geeks.” *Panayotis Vryonis* (blog), August 27, 2013. https://medium.com/@vrypan/explaining-public-key-cryptography-to-non-geeks-f0994b3c2d5.

“WFP Introduces Iris Scan Technology To Provide Food Assistance To Syrian Refugees In Zaatari | World Food Programme.” Accessed April 13, 2019. https://www1.wfp.org/news/wfp-introduces-innovative-iris-scan-technology-provide-food-assistance-syrian-refu.

“What Are MD5, SHA-1, and SHA-256 Hashes, and How Do I Check Them?” Accessed March 31, 2019. https://www.howtogeek.com/67241/htg-explains-what-are-md5-sha-1-hashes-and-how-do-i-check-them/.

“What Is a Smart Contract? - Definition from Techopedia.” Accessed April 1, 2019. https://www.techopedia.com/definition/32499/smart-contract.

“What Is Hashing? Under The Hood Of Blockchain - Blockgeeks.” Accessed March 31, 2019. https://blockgeeks.com/guides/what-is-hashing/.

“What’s A Merkle Tree? Komodo’s Guide To Understanding Merkle Trees.” *Komodo* (blog), July 19, 2018. https://komodoplatform.com/whats-merkle-tree/.

“Why Cutting Foreign Aid Benefits Terrorists.” Council on Foreign Relations. Accessed April 17, 2019. https://www.cfr.org/blog/why-cutting-foreign-aid-benefits-terrorists.

World Identity Network, London School of Economics, and UNOPS. “TURNING INVISIBLE CHILDREN INTO INVINCIBLE ONES.” Accessed April 23, 2019. https://win.systems/wp-content/uploads/2018/09/blockchain-for-humanity-1.pdf.

N.d.

N.d.

Biography

Hasan Syed was born in South Florida and lived there until moving to Plano, Texas 14 years later. He enrolled at The University of Texas at Austin in 2015, double majoring in Finance and the Plan II Honors program. During his time at UT, he pursued minors in Arabic and Spanish and studied at the Comillas Pontifical University (ICADE) in Madrid, Spain in the Spring of 2018. Hasan involved himself in the Clements Center for National Security, Tejas Club, Undergraduate Business Council, Plan II KIPP Tutoring, and disc-jockeyed at UT's KVRX Radio Station. He graduated in May 2019, and plans to join Evercore in the summer as an Investment Banking Analyst in their Mergers and Acquisitions group at their global headquarters in New York, New York.